Université de Montréal

FOUILLES, SAISIES ET PERQUISITIONS DE DONNÉES INFORMATIQUES : ATTENTE RAISONNABLE DE VIE PRIVÉE ET INFONUAGIQUE

par Laura Ellyson

Faculté de droit

Mémoire présenté en vue de l'obtention de grade de maître
en droit (LLM) (option générale)

Juin 2018

Résumé

L'article 8 de la *Charte canadienne des droits et libertés* prévoit que « chacun a droit à la protection contre les fouilles, les perquisitions ou les saisies abusives ». Cette disposition a fait couler beaucoup d'encre depuis son adoption, mais également plus récemment en raison de son application aux nouvelles technologies. En effet, dans les 20 dernières années, la Cour suprême du Canada a adapté les principes généraux découlant des fouilles, saisies et perquisitions aux réalités informatiques nouvelles, notamment l'ordinateur et le cellulaire.

Toutefois, l'émergence de nouvelles technologies est un phénomène qui ne cesse jamais. L'essor de l'infonuagique, ce modèle d'utilisation d'Internet qui permet l'accès à des services à distance, incluant notamment la sauvegarde de données sur des serveurs délocalisés, nous force à revoir la protection constitutionnelle qui peut être accordée aux données personnelles des individus. À travers l'étude des principes généraux applicables aux fouilles, saisies et perquisitions traditionnelles et d'appareils électroniques, nous expliquerons pourquoi les données délocalisées sauvegardées grâce à l'infonuagique peuvent être protégées par l'article 8 de la *Charte*. Nous analyserons également les différentes autorisations judiciaires permettant leur saisie, de même que certains autres principes connexes, notamment le cryptage de données et la protection par mot de passe.

Mots-clés : *Droit criminel, Libertés fondamentales, Vie privée, Perquisitions, Preuve pénale, Preuve numérique, Infonuagique*

Abstract

Section 8 of the *Canadian Charter of Rights and Freedoms* provides that "everyone has the right to be secure against unreasonable search or seizure". This provision has been written about extensively since its adoption, but also more recently because of its application to new technologies. In fact, in the last 20 years, the Supreme Court of Canada has adapted the general principles arising from search and seizure law to new technological realities, including computers and cell phones.

However, the emergence of new technologies is a phenomenon that never stops. The rise of cloud computing, this model of Internet utilisation that allows access to remote services, including but not limited to data storage on delocalized servers, forces us to review the constitutional protection that can be granted to personal data. Through the study of the general principles applicable to traditional search and seizure, and search and seizure of electronic devices, we will explain why delocalized data saved using cloud computing can be protected by section 8 of the *Charter*. We will also analyze the various judicial authorizations available to obtain this data, as well as certain other related principles, including data encryption and password protection.

Keywords: *Criminal law, Fundamentals rights, Privacy, Seizures, Criminal evidence, Electronic evidence, Cloud computing*

TABLE DES MATIÈRES

Liste des annexes

Liste des abréviations

C.cr.	Code criminel
Charte	*Charte canadienne des droits et libertés*
FBI	*Federal Bureau of Investigation*
FSI	Fournisseur de service Internet
GRC	*Gendarmerie Royale du Canada*
IaaS	*Infrastructure as a Service* ou « infrastructure en tant que service »
LPRPDE	*Loi sur la protection des renseignements personnels et les documents électroniques*
NSA	*National Security Agency*
PaaS	*Platform as a Service* ou « plate-forme en tant que service »
SaaS	*Software as a Service* ou « logiciel en tant que service »

Avant-propos

Dans les dernières années, nous avons assisté à une véritable explosion de l'utilisation de l'infonuagique, ce modèle d'utilisation d'Internet qui permet l'accès à des services à distance, incluant notamment la sauvegarde de données sur des serveurs délocalisés. En effet, bien que plusieurs individus n'aient aucune connaissance de ce fait, plusieurs appareils ou applications utilisent le *nuage* afin de permettre à ces données d'être accessibles à partir de n'importe quel appareil connecté ayant les autorisations nécessaires. Cette pratique n'est pas sans conséquence pour les autorités policières qui, dans certains dossiers, voudront accéder à ces données délocalisées. Elle n'est pas sans conséquence non plus pour les individus désirant commettre des infractions qui sont, bien souvent, très au fait de la possibilité que ces données soient plus difficilement accessibles.

Ma curiosité personnelle pour la rencontre de ces deux univers que sont le droit criminel et l'informatique relève un peu du hasard. Toutefois, en tant qu'avocate ayant pratiqué en défense criminelle et en tant que chargée de cours à Polytechnique Montréal, je suis à même de constater que les grands défis auxquels fait face le droit criminel sont principalement reliés à l'essor des nouvelles technologies et à leur prolifération rapide à l'échelle mondiale.

N'ayant pas la prétention de tout savoir sur la question de l'infonuagique ou encore du droit criminel, ce mémoire se veut une réflexion sur le virage que doit prendre le droit criminel canadien afin de s'adapter aux nouvelles technologies. Il est important de réfléchir maintenant à ces questions plutôt que d'attendre qu'un véritable problème arrive. En fait, je crois que l'obstacle se pointe déjà le bout du nez à l'horizon et qu'il est impératif pour les acteurs du droit criminel canadien de trouver maintenant des solutions afin de se prémunir contre le risque que les nouvelles technologies rendent obsolètes les outils qui sont à la disposition de l'État afin de lutter contre la criminalité.

Laura Ellyson
31 octobre 2017

Introduction

« […] nous devons toujours rester conscient du fait que les moyens modernes de surveillance électronique, s'ils ne sont pas contrôlés, sont susceptibles de supprimer toute vie privée. »[1]

Le débat public entre le respect de la vie privée et la capacité de l'État d'enquêter et de lutter contre le crime ne date pas d'hier et ne risque pas d'être résolu de sitôt. Les partisans de ces deux positions respectives ont effectivement des arguments importants et pertinents à faire valoir afin de défendre ce qui semble, à leurs yeux, être davantage important dans le cadre d'une société libre et démocratique ; les uns faisant valoir des principes comme « la maison de chacun est pour lui son château et sa forteresse »[2] et les autres invoquant plutôt des principes de sécurité et de répression du crime. Comme le présente Steve Coughlan : « [t]here is a constant tension between the interest of the state to ensure the collective security of its subjects and the interest of those subjects in liberty and security »[3]. Cette dualité ressort par ailleurs également des écrits de la Cour suprême[4].

La *Charte canadienne des droits et libertés*[5] ainsi que la *Charte des droits et libertés de la personne*[6] contiennent des dispositions protégeant la vie privée des individus[7] dans un contexte large[8]. Bien que l'étude approfondie du concept de vie privée ne fasse pas partie du cadre de cette étude, il importe de rappeler que le droit à la vie privée est pertinent dans plusieurs sphères juridiques, y compris en matière criminelle et pénale où ce droit est en lien direct avec la capacité

---

[1] *R.* c. *Wong*, [1990] 3 R.C.S. 36.
[2] *R.* c. *Tessling*, [2004] 3 R.C.S. 341, par. 22, citant *Semayne's Case*, [1558-1774] All. E.R. Rep. 62 (1604), p. 63.
[3] Stephen Gerard COUGHLAN, *Criminal procedure*, 3 éd., coll. Essentials of Canadian law, Toronto, Irwin Law, 2016, p. 3.
[4] *Hunter* c. *Southam inc.*, [1984] 2 R.C.S. 145, 159-160; *Baron* c. *Canada*, [1993] 1 R.C.S. 416, 26; *R.* c. *Golden*, [2001] 3 R.C.S. 679, par. 46; *R.* c. *Araujo*, [2000] 2 R.C.S. 992, par. 22; *R.* c. *Mann*, [2004] 3 R.C.S. 59, par. 1, 15.
[5] *Charte canadienne des droits et libertés*, partie I de la *Loi constitutionnelle de 1982*, [annexe B de la *Loi de 1982 sur le Canada*, 1982, c. 11 (R.-U.)], [ci-après la Charte].
[6] *Charte des droits et libertés de la personne*, L.R.Q., c. C-12.
[7] *Charte canadienne des droits et libertés*, préc., note 5, art. 7; *Charte des droits et libertés de la personne*, préc., note 6, art. 5.
[8] Il est utile de remarquer ici que l'article 7 de la Charte ne mentionne pas expressément le droit à la vie privée. Toutefois, nous sommes en accord avec plusieurs auteurs à l'effet que les principes de justice fondamentaux incluent le droit à la protection de la vie privée. Voir notamment : Benoît PELLETIER, « La protection de la vie privée au Canada », (2001) 35 *R.J.T.* 485.

de l'État d'exercer certains pouvoirs d'enquête. Nous référons bien évidemment ici au pouvoir d'effectuer des fouilles, saisies et perquisitions.

L'article 8 de la *Charte* prévoit que « chacun a droit à la protection contre les fouilles, les perquisitions ou les saisies abusives »[9]. À travers les années d'existence de la *Charte*, cette disposition a été utilisée à maintes reprises afin d'examiner la légalité des intrusions de l'État dans la vie privée de ses citoyens, dans le cadre d'enquêtes criminelles, qu'il s'agisse de perquisitions dans un domicile, de fouilles corporelles ou de saisie de documents. Par ailleurs, plus récemment, nous avons assisté à un réexamen de cette disposition, dans le cadre du développement de nouvelles technologies.

Dès 1990, la Cour suprême du Canada a commencé à se pencher sur le lien entre cette disposition et les nouvelles technologies utilisées par les policiers[10]. Toutefois, depuis 2010, nous assistons à une augmentation notable du nombre de décisions dans ce domaine, surtout en ce qui concerne les ordinateurs[11]. En effet, l'utilisation massive et répandue des ordinateurs a, en quelque sorte, enclenché cette étude de l'application de l'article 8 de la *Charte* aux nouvelles technologies. Il est maintenant rare qu'un individu ne possède aucun appareil électronique, qu'il s'agisse d'un ordinateur, d'une tablette, d'un téléphone intelligent ou encore d'une montre connectée. Tous ces appareils peuvent, le cas échéant, contenir des informations essentielles à une enquête criminelle.

Le recours croissant à l'Internet est également au cœur de ce débat. Peu de foyers canadiens sont maintenant hors ligne, c'est-à-dire qu'ils n'ont pas accès à l'Internet[12]. Ces considérations sont nécessairement au centre des enquêtes criminelles, que ce soient des enquêtes en matière

---

[9] *Charte canadienne des droits et libertés*, préc., note 5, art. 8.
[10] *R.* c. *Wong*, préc., note 1; *R.* c. *Duarte*, [1990] 1 R.C.S. 30.
[11] Nous fixons le point de départ de cette vague à l'arrêt *R.* c. *Morelli*, [2010] 1 R.C.S. 253.
[12] CANADIAN INTERNET REGISTRATION AUTHORITY, « Internet use in Canada », *Canadian Internet Registration Authority (CIRA)* (2 décembre 2016), en ligne : Cira <https://cira.ca/factbook/domain-industry-data-and-canadian-Internet-trends/internet-use-canada> (consulté le 20 octobre 2017).

de cybercriminalité[13] ou encore simplement des enquêtes où un élément de preuve peut se retrouver en format électronique.

La façon dont les Canadiens utilisent l'Internet et leurs ordinateurs est également en plein changement. En effet, de plus en plus de Canadiens utilisent des services d'infonuagique[14] (aussi connu sous le vocable anglophone de *cloud computing*[15]), c'est-à-dire qu'ils utilisent des services en ligne afin, notamment, de sauvegarder des données sur un serveur délocalisé, pouvant appartenant à un tiers, souvent une entreprise située à l'étranger. Les données ne se trouvent donc plus dans l'ordinateur du suspect ou de la personne sous enquête, mais bien sur un serveur qui peut être situé à n'importe quel endroit sur la planète[16]. Ce serveur va souvent être désigné sous le vocable de *nuage* (ou *cloud* en anglais), puisque les données peuvent être accédées à partir de n'importe quel appareil électronique possédant une connexion Internet. Une importante proportion d'internautes utilise ce genre de service, parfois sans même le savoir.

Cette utilisation d'Internet soulève des questions importantes en matière de vie privée, mais également en matière d'enquêtes criminelles. En effet, il n'est pas intuitif de déterminer de quelle manière l'article 8 de la *Charte* s'applique à l'infonuagique et aux données situées sur le *nuage*. Par ailleurs, peu de décisions canadiennes en droit criminel ont été recensées à ce jour

---

[13] L'étude approfondie de la cybercriminalité ne fait pas partie du cadre de ce mémoire puisque la découverte de preuve électronique n'est pas seulement pertinente dans des dossiers de cybercriminalité. Toutefois, cela sera bien souvent le cas, en raison de la nature même de ces infractions dites de cybercriminalité. Ainsi, il est utile de spécifier que la cybercriminalité inclut les crimes où l'ordinateur est l'objet même du crime (pensons ici aux infractions de méfait de données ou d'utilisation non-autorisée de services d'ordinateur, prévues au Code criminel, donc des infractions qui se déroule entièrement dans le monde virtuel, souvent désignées sous le vocal de piratage informatique), ou encore les crimes où l'ordinateur est l'outil du crime (des crimes où l'ordinateur facilite la commission de l'infraction ou encore des crimes traditionnels qui ont maintenant parfois une portée informatique). Voir à ce sujet : Laura ELLYSON et Annie EMOND, « Cybercriminalité : développements jurisprudentiels et perquisitions informatiques », dans *Repères*, septembre 2014, EYB2014REP1575.

[14] Louis COLUMBUS, « Roundup Of Cloud Computing Forecasts, 2017 » (29 avril 2017), en ligne : Forbes <https://www.forbes.com/sites/louiscolumbus/2017/04/29/roundup-of-cloud-computing-forecasts-2017/#5d7958b731e8> (consulté le 20 octobre 2017).

[15] OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, « infonuagique », en ligne : <http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=26501384> (consulté le 20 octobre 2017); Le terme anglophone *cloud computing* aurait été créé par Eric Schmidt, le PDG de l'entreprise Google, en 2006. Jacob M. SMALL, « Storing Documents in the Cloud: Toward an Evidentiary Privilege Protecting Papers and Effects Stored on the Internet », (2013) 23 *George Mason Univ. Civ. Rights Law J.* 255, 258.

[16] Ces serveurs sont souvent désignés sous les termes de *nuage* ou de *cloud*. Les deux termes seront donc utilisés dans le cadre de ce mémoire.

sur ce sujet, bien qu'il soit inévitable que des policiers se heurteront, tôt ou tard, à un problème d'accès au *nuage* d'un individu sous enquête, en raison de la prévalence de cette technologie.

En analysant l'évolution du droit contre les fouilles, perquisitions ou saisies abusives, nous tenterons de déterminer comment adapter celui-ci à l'infonuagique. Nous amorcerons ainsi notre analyse au chapitre 1 avec les principes généraux applicables aux fouilles, saisies et perquisitions, en nous attardant spécifiquement sur la question d'attente raisonnable de vie privée, qui constitue le point de départ d'une analyse fondée sur l'article 8 de la *Charte*. Nous examinerons également les diverses situations où une fouille peut avoir lieu sans autorisation préalable, ainsi que les différentes autorisations judiciaires prévues au *Code criminel*[17]. Nous conclurons notre premier chapitre avec l'analyse de la violation de l'article 8 de la *Charte* et du remède approprié, soit l'exclusion de preuve en vertu de l'article 24(2) de la *Charte*.

Au chapitre 2, nous examinerons plus spécifiquement les saisies de données informatiques, en nous attardant sur la jurisprudence récente de la Cour suprême rendue sur la question. Nous examinerons également certaines considérations techniques applicables aux saisies de données informatiques, telle que la création d'une copie miroir des données afin que celles-ci puissent être analysées. Certains cas problématiques – soit le cas des données protégées par mot de passe et par cryptage et la problématique de l'application de la théorie des « objets bien en vue » aux données informatiques – seront également considérés.

Finalement, au chapitre 3, après avoir expliqué certaines caractéristiques techniques applicables au *nuage*, nous appliquerons les principes dégagés lors des deux premiers chapitres au cas des données délocalisées, c'est-à-dire les données sauvegardées grâce à l'infonuagique. Nous démontrerons ainsi que ces données méritent la même protection que les données se trouvant dans un ordinateur, puisque les citoyens canadiens possèdent une attente raisonnable de vie privée à leur égard. Nous déterminerons ensuite les diverses ordonnances judiciaires applicables, selon différents scénarios, afin que les forces de l'ordre puissent accéder à de telles

[17] *Code criminel*, L.R.C. 1985, c. C-46 [ci-après C.cr.].

données. Certaines considérations techniques applicables au *nuage* seront alors examinées, de même qu'un survol des considérations de juridiction sera effectué.

Chapitre 1 – Les principes généraux applicables aux fouilles, saisies et perquisitions

Avant l'adoption de la *Charte* en 1982, la *common law* offrait une certaine protection contre les fouilles, saisies ou perquisitions effectuées par les autorités[18]. Cette protection était alors fondée sur le droit de propriété que possède chaque individu sur ses biens et également sur le droit de se protéger contre une intrusion[19]. Comme mentionné il y a déjà plusieurs années par James A. Fontana : « [n]othing in English law, the fountainhead of our own legal heritage, has been held to be so sacred as the inviolability of a man's home or premises »[20].

Bien que plusieurs principes de *common law* s'appliquent encore aujourd'hui en droit criminel, l'article 8 de la *Charte* est maintenant la source principale de recours fondée sur les fouilles, saisies ou perquisitions. La protection offerte par cette disposition est plus large que celle prévue par la *common law*, notamment en n'étant pas fondée sur le droit de se défendre contre une intrusion.

Nous allons commencer notre analyse par une revue des principes de base bien établis en matière de fouilles, saisies et perquisitions.

Section 1.1 La protection offerte par l'article 8 de la *Charte*

1.1.1 La définition des termes fouilles, saisies et perquisitions

Il est utile d'entreprendre notre analyse de l'article 8 de la *Charte* en définissant les termes principaux utilisés, soit « les fouilles, les perquisitions ou les saisies »[21]. En effet, selon la Cour dans la décision *Evans*, « tout type d'enquête gouvernementale ne constituera pas forcément, sur le plan constitutionnel, une "fouille ou perquisition" »[22]. Ainsi, et comme nous le verrons en

---

[18] *Hunter* c. *Southam inc.*, préc., note 4, 157; W.J. Garry BRACKEN, « Federal Law Relating to Search and Seizure », (1974) 23 *Univ. N. B. Law J.* 53.
[19] *Hunter* c. *Southam inc.*, préc., note 4, 157.
[20] James A. FONTANA, *The Law of Search Warrants in Canada*, Toronto, Butterworths, 1974, p. 1.
[21] *Charte canadienne des droits et libertés*, préc., note 5, art. 8.
[22] *R.* c. *Evans*, [1996] 1 R.C.S. 8, par. 11.

détail plus loin, il y aura fouille, saisie ou perquisition seulement lorsqu'un individu jouit d'une attente raisonnable de vie privée[23]. Cette qualification revêt une importance particulière puisqu'il s'agit de la première étape de l'analyse fondée sur l'article 8 de la *Charte*[24]. En effet, si un individu ne peut prouver qu'il jouissait d'une attente raisonnable de vie privée, il ne pourra y avoir violation de l'article 8 de la *Charte*[25].

De plus, il importe de souligner que ces termes ne doivent pas être assimilés à des synonymes. En effet, chacun de ces termes possède un sens précis, qui peut être distingué des autres. Ainsi, une fouille vise habituellement le fait de fouiller une personne, que ce soit ses vêtements ou son corps lui-même[26]. La saisie vise les cas où « les autorités prennent quelque chose appartenant à une personne sans son consentement »[27] lorsque cette personne peut « raisonnablement s'attendre à ce qu'on préserve le caractère confidentiel »[28] de cette chose. La saisie a également été définie en tant qu'« appropriation par un pouvoir public d'un objet appartenant à une personne contre le gré de cette personne »[29], faisant en sorte qu'un *subpoena duces tecum* puisse être assimilé à une saisie. Par ailleurs, la Cour suprême a souligné qu'une interprétation large du terme saisie doit être privilégiée, afin de ne pas détourner l'article 8 de la *Charte* de sa finalité. Ainsi, il ne faut pas seulement examiner le procédé employé par l'État lui-même afin de déterminer s'il s'agit d'une saisie, mais également le contexte dans lequel le procédé a été appliqué[30]. Finalement, la perquisition est habituellement un terme réservé à la recherche d'éléments de preuve dans un lieu donné, tel que la perquisition d'une résidence.

Ainsi, il y aura généralement fouille et saisie (ou perquisition et saisie), le premier terme visant la recherche des éléments de preuve alors que le second terme vise plutôt le fait de prendre les objets ainsi trouvés. Par ailleurs, la Cour suprême a jugé utile de préciser que ces termes doivent

---

[23] *Hunter* c. *Southam inc.*, préc., note 4, 159; *Schreiber* c. *Canada*, [1998] 1 R.C.S. 841, par. 18; *R.* c. *MacDonald*, [2014] 1 R.C.S. 37, par. 25; *R.* c. *A.M.*, [2008] 1 R.C.S. 569, par. 8.
[24] Voir notamment *R.* c. *Gomboc*, [2010] 3 R.C.S. 211, par. 20.
[25] S. G. COUGHLAN, préc., note 3, p. 71.
[26] Tel que la fouille à nu pratiquée dans la décision *R.* c. *Golden*, préc., note 4.
[27] *R.* c. *Dyment*, [1988] 2 R.C.S. 417, 431.
[28] *R.* c. *Borden*, [1994] 3 R.C.S. 145, 160.
[29] *Thomson Newspapers Ltd.* c. *Canada (Directeur des enquêtes et recherche, Commission sur les pratiques restrictives du commerce)*, [1990] 1 R.C.S. 425, 493.
[30] *Québec (Procureur général)* c. *Laroche*, [2002] 3 R.C.S. 708, par. 53.

être lus de manière disjonctive, c'est-à-dire que la saisie en elle seule peut être abusive, tandis que la fouille ou la perquisition peut ne pas l'être[31]. Certaines situations demeurent toutefois plus difficiles à placer dans une catégorie particulière, notamment lorsqu'il s'agit de collecte de renseignements[32].

Malgré tout, et ce afin d'alléger le texte, ces termes seront parfois utilisés de manière interchangeable, à moins qu'une distinction s'impose.

1.1.2 Les principes découlant de l'analyse de l'article 8 de la Charte

Lorsque la Cour suprême du Canada a voulu examiner la nouvelle protection offerte par l'article 8 de la *Charte*, elle s'est tout d'abord inspirée de la jurisprudence américaine portant sur le Quatrième Amendement de la Constitution américaine[33]. Ainsi, il a été déterminé qu'à l'instar de son pendant américain, l'article 8 de la *Charte* protège les personnes et non les lieux[34]. La Cour a également déterminé que l'objectif poursuivi par cette disposition est « de protéger les particuliers contre les intrusions injustifiées de l'État dans leur vie privée »[35], quoique la vie privée ne soit pas le seul objectif poursuivi[36]. On peut ainsi dire que l'article 8 prévoit une « interdiction qui est faite au gouvernement de s'intéresser de trop près à la vie des citoyens [ce qui] touche à l'essence même de l'État démocratique »[37].

Bien que le droit à la vie privée fût à l'origine fondé, tel que nous l'avons vu, sur des notions de droit de propriété[38], la *Charte* doit être interprétée de façon large et libérale, de façon à évoluer avec la société canadienne[39]. Ainsi, la vie privée ne réfère plus uniquement à des revendications

---

[31] *R.* c. *Dyment*, préc., note 27, 431, citant *Milton* v. *The Queen* (1985), 16 C.R.R. 215.
[32] Les termes « fouille et perquisition » semblent utilisés de manière interchangeable pour plusieurs situations dans la jurisprudence sur le sujet.
[33] Comme le souligne un auteur, bien que le texte de la Charte en lui-même soit plutôt basé sur des textes européens, l'interprétation de la Charte est surtout fondée sur la jurisprudence américaine. Jerome ATRENS, « A Comparison of Canadian and American Constitutional Law Relating to Search and Seizure », (1994) 1 *Southwest. J. Law Trade Am.* 29, 30.
[34] *Hunter* c. *Southam inc.*, préc., note 4, 159.
[35] *Id.*
[36] J. ATRENS, préc., note 33, 34.
[37] *R.* c. *Dyment*, préc., note 27, 427-428.
[38] Voir aussi *R.* c. *Tessling*, préc., note 2, par. 16.
[39] *Hunter* c. *Southam inc.*, préc., note 15, 155; *R.* c. *Big M Drug Mart*, [1985] 1 R.C.S. 295, 344.

reliées à la propriété (ou revendications territoriales), mais également à des revendications « qui ont trait à la personne et celles qui sont faites dans le contexte informationnel »[40]. Par ailleurs, la vie privée « repose sur les valeurs "de dignité, d'intégrité et d'autonomie" »[41].

Dans la décision *Duarte*, la Cour suprême du Canada a défini la notion de vie privée comme « le droit du particulier de déterminer lui-même quand, comment et dans quelle mesure il diffusera des renseignements personnels le concernant »[42]. Il est maintenant convenu que la vie privée inclut plusieurs sphères distinctes. En effet, selon la Cour suprême :

> « […] la jurisprudence relative à l'art. 8 a évolué et reconnaît dorénavant plusieurs aspects du droit au respect de la vie privée, à savoir :
>
> > (i) le droit à la vie privée qui a trait à la personne, lequel protège l'intégrité corporelle et le droit de refuser toute palpation ou exploration corporelle;
> >
> > (ii) le droit à la vie privée qui a trait aux lieux, lequel comporte diverses attentes en matière de vie privée selon les lieux que nous occupons, le droit à la vie privée dans notre résidence commandant une protection plus grande parce qu'il s'agit du lieu où nos activités les plus intimes et privées se déroulent;
> >
> > (iii) le droit au respect du caractère privé des renseignements personnels, qui se définit comme « le droit revendiqué par des particuliers, des groupes ou des institutions de déterminer eux-mêmes le moment, la manière et la mesure dans lesquels des renseignements les concernant sont communiqués » (par. 23, citant A. F. Westin, *Privacy and Freedom* (1970), p. 7).
>
> Dans l'arrêt *Tessling*, la Cour reconnaît également que, même si elles fournissent des outils d'analyse utiles, ces catégories ne sont pas forcément étanches et peuvent se recouper. »[43]

Tel que mentionné en introduction et tel qu'il sera à nouveau question dans ce mémoire, l'analyse fondée sur l'article 8 de la *Charte* dépend en grande partie de la recherche d'équilibre entre la vie privée des citoyens et le devoir de répression du crime de l'État. Ainsi :

---

[40] *R.* c. *Dyment*, préc., note 27, 428.
[41] Pierre BÉLIVEAU et Martin VAUCLAIR, *Traité général de preuve et de procédure pénales*, 20e éd., Cowansville, Éditions Yvon Blais, 2013, par. 854; citant *R.* c. *Tse*, [2012] 1 R.C.S. 531, par. 21.
[42] *R.* c. *Duarte*, préc., note 10, 46.
[43] *R.* c. *Gomboc*, préc., note 24, par. 19.

> « L'analyse du droit au respect de la vie privée abonde en jugements de valeur énoncés du point de vue indépendant de la personne raisonnable et bien informée, qui se soucie des conséquences à long terme des actions gouvernementales sur la protection du droit au respect de la vie privée. »[44]

Tout comme la protection offerte par la *common law*, la *Charte* exige généralement qu'une autorisation préalable soit obtenue afin qu'une perquisition, fouille ou saisie soit jugée raisonnable, sous réserve de certaines exceptions qui seront brièvement étudiées ci-dessous. *A contrario*, une perquisition, fouille ou saisie effectuée sans mandat sera présumée abusive et il appartiendra alors à la partie voulant l'invoquer de prouver sa légalité[45]. Cette autorisation préalable pourra être décernée seulement s'il existe des motifs raisonnables de croire qu'une infraction a été commise et que la fouille, saisie ou perquisition pourra fournir des éléments de preuve en lien avec cette infraction[46]. Si une autorisation judiciaire a été obtenue, il appartiendra alors à la partie cherchant à faire invalider la fouille, saisie ou perquisition de prouver le caractère autrement abusif de celle-ci, selon la norme de preuve de la prépondérance des probabilités[47].

Lorsque l'existence d'une attente raisonnable de vie privée a été établie et qu'on peut donc qualifier la conduite étatique de fouille, saisie ou perquisition, la deuxième étape de l'analyse fondée sur l'article 8 de la *Charte* consiste en se demander si celle-ci a été effectuée de manière abusive ou non. Selon l'arrêt *Collins,* trois conditions doivent être remplies pour qu'une fouille ne soit pas considérée abusive : « a) elle doit être autorisée par la loi, b) la loi elle-même ne doit pas être abusive, et c) la fouille ne doit pas avoir été effectuée de manière abusive »[48]. Tel que mentionné, lorsque la fouille a été effectuée sans mandat, il appartiendra au ministère public de faire la preuve du respect de ces trois conditions, selon la prépondérance des probabilités[49].

---

[44] *R.* c. *Patrick*, [2009] 1 R.C.S. 579, par. 14.
[45] *Hunter* c. *Southam inc.*, préc., note 4, 161; *R.* c. *Feeney*, [1997] 2 R.C.S. 13, 78; *R.* c. *Paterson*, [2017] 1 R.C.S. 202, par. 46; *R.* c. *Collins*, [1987] 1 R.C.S. 265, 278; *R.* c. *Kokesh*, [1990] 3 R.C.S. 3, 15.
[46] *Hunter* c. *Southam inc.*, préc., note 4, 168. Le seuil est parfois moindre (soit les motifs raisonnables de soupçonner) pour certains types d'ordonnances de communication. Voir section 1.3.4 du présent mémoire.
[47] *R.* c. *Collins*, préc., note 45, 277; *R.* c. *Shin*, 2012 ONCA 707.
[48] *R.* c. *Collins*, préc., note 45, 278; Voir aussi *R.* c. *Stillman*, [1997] 1 R.C.S. 607, par. 25.
[49] *R.* c. *Buhay*, [2003] 1 R.C.S. 631, par. 32.

Pour la première condition, outre l'existence d'une autorisation judiciaire[50], un pouvoir de fouille établi par la *common law* peut constituer une justification valide pouvant légitimer une fouille[51], de même qu'une fouille effectuée avec le consentement de la personne visée. Par ailleurs, il importe de mentionner que même lorsqu'une autorisation judiciaire a été obtenue, la possibilité que l'ordonnance n'ait pas été du bon genre, ou du bon type, demeure[52]. Ainsi, cela équivaut à l'absence d'autorisation judiciaire, ce qui rend la perquisition ou fouille invalide.

En ce qui concerne la seconde condition, il importe de faire des distinctions entre une fouille autorisée par un pouvoir de *common law* et une fouille autorisée par une loi. Tout d'abord, pour les fouilles autorisées par une loi, le degré d'attente de vie privée d'un individu fera varier le degré de protection nécessaire[53]. Ainsi, lorsqu'un individu a une attente dite « normale » de vie privée, le test des « motifs raisonnables de croire », établi à l'article 487 C.cr., sera la norme[54]. Un degré d'attente plus faible pourrait se traduire par la norme des « motifs raisonnables de soupçonner », prévu notamment à l'article 487.018 C.cr.[55], tandis qu'un degré plus fort se traduirait par des conditions additionnelles, comme il est le cas pour les ordonnances d'interception de communications privées ou pour les mandats relatifs aux analyses génétiques[56]. Par ailleurs, la méthode d'émission de l'autorisation judiciaire est également pertinente. En effet, selon la décision *Hunter*, il faut que la personne qui autorise le mandat soit « en mesure d'agir de façon judiciaire »[57], bien qu'il ne soit pas nécessaire que celle-ci exerce la fonction de juge. Il faut également que cet individu ait une discrétion quant à l'émission du mandat[58]. En somme :

> « Ordinairement, la loi qui permet une fouille sera jugée constitutionnelle si elle prévoit un mécanisme d'autorisation préalable (un mandat) par une personne agissant judiciairement (habituellement un juge) se fondant sur l'existence de motifs raisonnables

---

[50] Celles-ci seront présentées à la section 1.3 du présent mémoire.
[51] *R.* c. *Stillman*, préc., note 49, par. 25. Voir section 1.1.3 pour plus de détails sur certains pouvoirs de fouille découlant de la *common law*.
[52] *R.* c. *Jones*, [2017] 2 R.C.S. 696, par. 57.
[53] S. G. COUGHLAN, préc., note 3, p. 142.
[54] *Id.*
[55] Soit l'ordonnance de communication – données financières.
[56] S. G. COUGHLAN, préc., note 3, p. 143-144.
[57] *Hunter* c. *Southam inc.*, préc., note 4, 162.
[58] *Baron* c. *Canada*, préc., note 4, 26; S. G. COUGHLAN, préc., note 3, p. 143.

> et probables, établis sous serment, de croire qu'un crime a été commis ou est commis et que la fouille permettra de découvrir des éléments de preuve particuliers. »[59]

Pour ce qui est de la légalité des fouilles autorisées par un pouvoir de *common law*, l'analyse applicable a été élaborée par la Cour d'appel d'Angleterre dans l'arrêt *Waterfield*[60]. Selon la Cour suprême :

> « [e]n pareil cas, le tribunal se demande d'abord si la conduite du policier à l'origine de l'atteinte entre dans le cadre général d'un devoir imposé à ce dernier par une loi ou par la *common law*. Si cette condition préliminaire a été satisfaite, le tribunal poursuit l'analyse et se demande si cette conduite, bien qu'elle respecte le cadre général du devoir en question, a donné lieu à un emploi injustifiable de pouvoirs afférents à ce devoir. »[61]

Selon la Cour, cette analyse doit être interprétée de manière restrictive, de manière à ne pas faire primer le devoir d'enquête des policiers sur toute autre considération à tout prix[62]. Ceci s'explique notamment puisque la *common law* doit être interprétée de manière compatible avec les enseignements de la *Charte*[63]. Cette étape de l'arrêt *Collins* renvoie directement à la recherche d'un équilibre entre les intérêts de l'État en matière de lutte contre le crime et les intérêts en matière de vie privée de ses citoyens[64].

Il est utile de spécifier que les deux premières étapes de l'analyse établie dans l'arrêt *Collins* sont souvent regroupées par les tribunaux[65].

Finalement, pour la troisième condition, il s'agit d'examiner la manière par laquelle la fouille a été effectuée par les policiers. En d'autres termes, à cette étape, les tribunaux doivent examiner la façon dont les autorités ont appliqué une loi ou un pouvoir de fouille de *common law* dans les circonstances précises du dossier sous étude[66]. Par exemple, dans la décision *Golden*, la majorité a conclu que les fouilles à nu pouvaient faire partie du pouvoir de fouille accessoire à une

---

[59] P. BÉLIVEAU et M. VAUCLAIR, préc., note 41, par. 890.
[60] *R.* v. *Waterfield*, [1963] 3 All. E.R. 659.
[61] *R.* c. *Mann*, préc., note 4, par. 24.
[62] *R.* c. *MacDonald*, préc., note 23, par. 38; citant *Renvoi sur l'écoute électronique*, [1984] 2 R.C.S. 697, 718-719.
[63] *R.* c. *Golden*, préc., note 4, par. 86.
[64] *R.* c. *Rodgers*, [2006] 1 R.C.S. 554, par. 27; qui renvoie à *Hunter* c. *Southam inc.*, préc., note 4, 159-160.
[65] Voir notamment *R.* c. *MacDonald*, préc., note 23, par. 31.
[66] *R.* c. *Thompson*, [1990] 2 R.C.S. 1111, 1146.

arrestation, à certaines conditions, mais que, dans les circonstances précises de cette affaire, la fouille n'avait pas été effectuée de manière raisonnable, notamment puisqu'elle avait été effectuée à l'extérieur d'un poste de police[67]. Ce critère de l'arrêt *Collins* a également été utilisé afin de se pencher sur la légalité des entrées dynamiques dans le cadre de perquisitions[68].

Par ailleurs, dans l'arrêt *Dyment*, la Cour nous rappelle que l'article 8 de la *Charte* vise également un objectif préventif, en raison du terme « protection » utilisé[69]. Ainsi, il ne s'agit pas seulement de réprimer, *a posteriori*, des fouilles, saisies ou perquisitions abusives, mais également de les prévenir[70]. Des règles claires doivent donc être établies afin que les forces de l'ordre sachent à quoi s'en tenir.

1.1.3 La notion d'attente raisonnable de vie privée

Dès la décision *Hunter c. Southam inc.*, la Cour suprême du Canada a abordé la notion d'attente raisonnable de vie privée[71] qui est à la base de toute analyse fondée sur l'article 8 de la *Charte canadienne*. En effet, et tel que mentionné précédemment, si la Cour conclut à l'absence d'une attente raisonnable de vie privée, la protection prévue par l'article 8 de la *Charte* ne s'appliquera tout simplement pas, puisque l'action étatique ne pourra alors être considérée comme une fouille, saisie ou perquisition.

Par ailleurs, bien que les tribunaux examinent souvent la notion d'attente de vie privée que lorsqu'il est temps de déterminer si le comportement étatique se qualifie comme une fouille, saisie ou perquisition, cette notion aura également un rôle à jouer ultérieurement. En effet, l'attente de vie privée sera également utile lorsqu'il sera temps de vérifier si ce comportement étatique était raisonnable. À cette seconde étape, le degré d'attente de vie privée sera pertinent[72],

---

[67] *R.* c. *Golden*, préc., note 4, par. 107.
[68] *R.* c. *Cornell*, [2010] 2 R.C.S. 142.
[69] *R.* c. *Dyment*, préc., note 27, 430.
[70] *Hunter* c. *Southam inc.*, préc., note 4, 160.
[71] *Id.*, 159.
[72] Ainsi, plus l'attente de vie privée est élevée, comme pour une maison ou le corps humain, plus la raisonnabilité de la technique d'enquête sera examinée de manière sévère. A contrario, si l'attente de vie privée est moindre, comme pour une voiture, plus la technique d'enquête a de chance d'être considérée comme raisonnable. Voir James A.Q. STRINGHAM, « Reasonable Expectations Reconsidered: A Return to the Search for a Normative Core for

tandis qu'à la première étape, il s'agit seulement de vérifier si une telle attente existe, et ce, peu importe si l'attente est plus ou moins élevée[73]. À la première étape, le fardeau à remplir pour l'individu réclamant la protection de l'article 8 de la *Charte* ne devrait pas être indûment élevé, puisqu'il s'agit simplement de prouver s'il existe une attente raisonnable de vie privée[74]. Par ailleurs, si le fardeau était trop difficile à remplir, il se produirait une situation d'impunité pour les représentants de l'État, puisque leur comportement serait alors hors du champ de contrôle des tribunaux : « [t]he whole point of section 8 is to balance competing interests, but to find no reasonable expectation of privacy is to remove any possibility of balancing. »[75]

La Cour suprême dans la décision *Hunter* n'a toutefois pas spécifiquement abordé la manière dont cette attente raisonnable de vie privée doit être évaluée; cette notion s'est plutôt précisée dans les arrêts subséquents de la Cour. Nous allons donc amorcer l'analyse de cette notion fondamentale en examinant ces différents arrêts qui proposent des approches ou analyses afin de déterminer s'il y a bel et bien existence d'une attente raisonnable de vie privée.

1.1.3.1 L'analyse fondée sur le risque

En 1990, la Cour suprême a rejeté l'analyse fondée sur le risque dans la décision *Duarte*[76]. Dans cette affaire, où il était question d'enregistrement de conversations privées avec le consentement d'une des parties à la conversation, la Cour a rejeté la prétention qu'il n'y a pas d'attente raisonnable de vie privée lorsque nous échangeons avec un tiers, même s'il y a un risque que celui-ci rapporte éventuellement nos paroles à un représentant de l'État. Selon la Cour :

> « L'idée que nous sommes protégés contre les interceptions arbitraires des communications privées perd tout fondement réel dès qu'il est admis que l'État est entièrement libre de les enregistrer à la seule condition d'avoir obtenu le consentement

---

Section 8? », (2005) 23 *Crim. Rep.* 245; Lisa M AUSTIN, « Information Sharing and the "Reasonable" Ambiguities of Section 8 of the Charter », (2007) 57 *U Tor. LJ* 499, 503.

[73] S. G. COUGHLAN, préc., note 3, p. 71; Lisa M. AUSTIN, « Is Consent the Foundation of Fair Information Practices? Canada's Experience under PIPEDA », (2006) 56 *Univ Tor. LJ* 181; J. A. Q. STRINGHAM, préc., note 73; James A FONTANA et David KEESHAN, *The law of search and seizure in Canada*, 9e éd., Toronto, LexisNexis, 2015, p. 21.

[74] S. G. COUGHLAN, préc., note 3, p. 73.

[75] *Id.*

[76] *R.* c. *Duarte*, préc., note 10.

> d'un des participants à la communication. […] Je conclus donc que l'analyse fondée sur le risque adoptée par la Cour d'appel aboutit logiquement à l'anéantissement de toute aspiration au respect de la vie privée. »[77]

Ainsi, bien que la conversation avec un policier agissant comme indicateur ne soit pas une fouille, saisie ou perquisition, l'enregistrement de cette conversation en est une[78]. Autrement dit, le risque qu'un individu dévoile à l'État les propos que nous tenons n'est pas suffisant pour éliminer notre attente de vie privée quant au fait que ces propos ne seront pas enregistrés ou autrement sauvegardés par l'État. Cette approche a été confirmée dans la décision *Wong*[79] en 1990 et plus récemment dans la décision *Marakah*[80].

Dans *Marakah*, la Cour s'est penchée sur l'existence d'une attente raisonnable de vie privée envers des messages textes se trouvant dans le téléphone du récipiendaire (donc des messages textes arrivés à destination). La majorité, sous la plume de l'honorable juge en chef McLachlin, tel qu'était alors son titre, a conclu que, dans certains cas, il sera possible qu'un individu possède une attente raisonnable de vie privée envers de tels messages, et ce, bien qu'il y ait un risque que le récipiendaire dévoile les messages aux policiers[81]. En ce sens, elle conclut qu'« [a]ccepter le risque qu'un interlocuteur divulgue une conversation électronique ne revient pas à accepter le risque différent que l'État s'immisce dans une conversation électronique non divulguée. »[82]

Bien que l'analyse fondée sur le risque ait été rejetée de manière non équivoque, il demeure que celle-ci semble parfois refaire surface. En effet, la dissidence du juge Moldaver dans la décision *Marakah* conclut à l'absence d'une attente raisonnable de vie privée dans les messages textes arrivés à destination, en raison de l'absence de contrôle du destinataire sur ceux-ci. Bien que réitérant que l'approche fondée sur le risque a été rejetée dans la décision *Duarte*, le juge Moldaver semble considérer que le risque que le récipiendaire des messages textes les dévoile

---

[77] *Id.*, 47-48.
[78] *Id.*, 57; François BLANCHETTE, *L'expectative raisonnable de vie privée et les principaux contextes de communications dans Internet*, mémoire de maîtrise, Montréal, Faculté des études supérieures, Université de Montréal, 2001, p. 22.
[79] *R.* c. *Wong*, préc., note 1, 45.
[80] *R.* c. *Marakah*, [2017] 2 R.C.S. 608.
[81] *Id.*, par. 4-5, 80.
[82] *Id.*, par. 41.

aux autorités a un rôle à jouer dans la détermination de l'attente de vie privée de l'expéditeur des messages[83]. Il a été suggéré que le recours à cette approche, malgré son rejet clair, résulte notamment de sa facilité d'application[84], qui serait plus intuitive que l'analyse contextuelle qui est maintenant utilisée.

Cette notion de risque sera particulièrement pertinente lorsqu'il sera question d'étudier la notion d'attente de vie privée dans le contexte de l'infonuagique, puisque certaines juridictions ou certains courants s'appuient sur cette théorie afin de nier l'existence d'une atteinte raisonnable de vie privée à l'égard de données sauvegardées chez une tierce personne.

1.1.3.2 L'analyse contextuelle

À la suite du rejet de l'analyse fondée sur le risque[85], la Cour a plutôt adopté une approche contextuelle. Selon cette approche, l'ensemble des circonstances doit être considéré afin de déterminer si une attente raisonnable de vie privée existe. D'abord utilisée dans les arrêts *Colarusso*[86] et *Wong*[87], cette approche s'est ensuite raffinée.

Dans *Edwards*, une affaire de possession de drogue en vue d'en faire le trafic, la Cour a proposé une série de facteurs, provenant d'une décision américaine, pouvant être considérés lors de la détermination de l'attente de vie privée d'un individu :

> « Les facteurs qui peuvent être pris en considération dans l'appréciation de l'ensemble des circonstances incluent notamment :
>
> (i) la présence au moment de la perquisition ;
> (ii) la possession ou le contrôle du bien ou du lieu faisant l'objet de la fouille ou de la perquisition ;
> (iii) la propriété du bien ou du lieu ;

---

[83] *Id.*, par. 129.
[84] S. G. COUGHLAN, préc., note 3, p. 75-76.
[85] Il est utile de préciser que certains auteurs parlent d'une étape intermédiaire dans l'approche utilisée par la Cour suprême dans l'analyse de la notion d'attente raisonnable de vie privée. En effet, après avoir rejeté l'approche fondée sur le risque, certains auteurs opinent que la Cour suprême a adopté une « approche de principe », mettant dans des catégories précises certains comportements de l'État. Voir F. BLANCHETTE, préc., note 79.
[86] *R.* c. *Colarusso*, [1994] 1 R.C.S. 20, 54.
[87] *R.* c. *Wong*, préc., note 1, 62.

(iv) l'usage historique du bien ou de l'article ;
(v) l'habilité à régir l'accès au lieu, y compris le droit d'y recevoir ou d'en exclure autrui ;
(vi) l'existence d'une attente subjective en matière de vie privée ;
(vii) le caractère raisonnable de l'attente, sur le plan objectif. »[88]

En appliquant ces facteurs au cas de M. Edwards, la Cour a conclu qu'il ne pouvait prétendre avoir une attente raisonnable de vie privée à l'égard de l'appartement d'une amie chez qui il avait dissimulé des stupéfiants. Mentionnant que la liste de facteurs n'est pas exhaustive, la Cour a tout de même noté qu'aucun des facteurs mentionnés ne s'appliquait dans le cas de M. Edwards, ce qui militait contre la reconnaissance d'une attente raisonnable de vie privée[89].

Par la suite, quelques années plus tard, la Cour s'est penchée sur l'expectative de vie privée dans un cas ayant principalement trait à la sphère informationnelle de la vie privée[90]. Dans la décision *Tessling*, la Cour a dû examiner le cas de l'imagerie thermale FLIR, qui permet de capter la chaleur s'échappant d'un édifice. Pour tenir compte du contexte particulier de l'affaire, la Cour a adapté les critères de l'arrêt *Edwards* au contexte informationnel du dossier. Ainsi, la Cour a établi certains critères devant être considérés pour décider du caractère raisonnable de l'attente de vie privée d'un individu en matière informationnelle, notamment de savoir « si des tiers possédaient déjà les renseignements [et si,] dans l'affirmative, ces renseignements étaient […] visés par une obligation de confidentialité »[91]. Ces critères ont également été repris dans l'arrêt *Patrick*[92].

Les critères pertinents vont donc varier d'un cas à l'autre, notamment selon la sphère de vie privée qui est en jeu. Afin d'englober toutes ces particularités, une analyse en quatre étapes est maintenant suivie par les tribunaux. Tel que résumé dans l'arrêt *Spencer* :

> « La grande variété et le nombre important de facteurs pouvant être pris en considération pour évaluer les attentes raisonnables en matière de respect de la vie privée peuvent être

---

[88] *R.* c. *Edwards*, [1996] 1 R.C.S. 128, par. 45.
[89] *Id.*, par. 46.
[90] Voir section 1.1.2 pour les trois différentes sphères de la vie privée.
[91] *R.* c. *Tessling*, préc., note 2, par. 32. Cette question serait déterminante lorsqu'il s'agira d'examiner l'attente de vie privée à l'égard de données situées sur un serveur appartenant à un tiers.
[92] *R.* c. *Patrick*, préc., note 44, par. 26 et suivants.

> regroupés, par souci de commodité, en quatre grandes catégories : (1) l'objet de la fouille ou de la perquisition contestée; (2) le droit du demandeur à l'égard de l'objet; (3) l'attente subjective du demandeur en matière de respect de sa vie privée relativement à l'objet; et (4) la question de savoir si cette attente subjective en matière de respect de la vie privée était objectivement raisonnable, eu égard à l'ensemble des circonstances […]. »[93]

Il est important de noter qu'aucun facteur n'est plus important qu'un autre. Il s'agit d'une analyse contextuelle, qui variera nécessairement d'un cas à l'autre. De plus, il convient également de rappeler que ce sera l'individu contestant la validité de la fouille qui aura le fardeau de convaincre la Cour qu'une attente raisonnable de vie privée existe, selon le fardeau de la prépondérance des probabilités[94].

A) L'objet de la fouille

La détermination de l'objet de la fouille ou de la perquisition peut sembler être une étape banale à première vue. En effet, dans bien des cas, il sera plutôt facile de déterminer quel est l'objet de la fouille. Toutefois, lorsqu'il s'agit de recherche de renseignements personnels, il peut être plus ardu de bien cerner l'objet de la fouille. Ainsi,

> « L'objet de la fouille doit être défini de manière fonctionnelle et non en fonction d'actes matériels, de l'emplacement physique ou des modalités de la transmission. Ainsi que le juge Doherty l'a expliqué dans l'arrêt *R. c. Ward*, 2012 ONCA 660, 112 O.R. (3d) 321, au par. 65, lorsqu'il est appelé à préciser l'objet de la fouille ou de la perquisition contestée, le tribunal ne doit pas adopter une approche [TRADUCTION] "restrictive portant sur les actes commis ou l'espace envahi, mais doit plutôt adopter une approche qui tient compte de la nature des droits en matière de vie privée auxquels l'action de l'État pourrait porter atteinte". Dans l'arrêt *Spencer*, au par. 26, le juge Cromwell a repris ces propos à son compte, ajoutant que les tribunaux devaient adopter "une approche large et fonctionnelle, en examinant le lien entre la technique d'enquête utilisée par la police et l'intérêt en matière de vie privée qui est en jeu" et que les tribunaux devaient examiner "non seulement la nature des renseignements précis recherchés, mais aussi la nature des renseignements qui sont ainsi révélés". Pour reprendre la formule employée par le juge Doherty dans *Ward*, la mission du tribunal consiste à déterminer "ce que la police recherchait vraiment" (par. 67). »[95]

---

[93] *R.* c. *Spencer*, [2014] 2 R.C.S. 212, par. 18; Voir aussi *R.* c. *Cole*, [2012] 3 R.C.S. 34, par. 40.
[94] J. A. FONTANA et D. KEESHAN, préc., note 74, p. 18.
[95] *R.* c. *Marakah*, préc., note 81, par. 15.

En appliquant ces principes, la Cour a déterminé dans *Marakah* que l'objet de la fouille n'était pas le téléphone saisi, mais bien la conversation électronique s'y trouvant[96]. De la même manière, dans *Cole*, il a été décidé que l'objet de la fouille n'était pas l'ordinateur lui-même, mais bien les données qu'il contenait[97]. La protection offerte par l'article 8 de la *Charte* vise donc les renseignements biographiques des individus, notamment des renseignements « tendant à révéler des détails intimes sur le mode de vie et les choix personnels des individus »[98]. On ne doit donc pas s'arrêter à ce qui semble, à première vue, être l'objet recherché par l'État, mais bien ce qui est susceptible d'être révélé sur un individu par la technique d'enquête. Ces principes ont également permis de déterminer que dans le cas d'une demande formulée à un fournisseur de service Internet (FSI) requérant les informations d'un usager associé à une adresse IP spécifique, le véritable objet de la fouille est l'identité de l'abonné, par rapport à une utilisation particulière de ces services Internet, non pas simplement le nom et l'adresse de celui-ci[99].

B) Le droit du demandeur à l'égard de l'objet

En ce qui concerne le droit du demandeur à l'égard de l'objet, il pourrait souvent être facile d'en déduire l'existence lorsque des détails intimes sont révélés par la méthode d'enquête. Ce fut notamment le cas dans *Marakah*, où la majorité a conclu à l'existence d'un intérêt direct dans la conversation électronique (messages textes) faisant l'objet de la fouille[100]. Par ailleurs, bien qu'un droit de propriété puisse faciliter la preuve d'une attente de vie privée, l'absence d'un tel droit n'est pas fatale[101].

---

[96] *Id.*, par. 17.
[97] *R.* c. *Cole*, préc., note 94, par. 41.
[98] *R.* c. *Plant*, [1993] 3 R.C.S. 281, 293.
[99] *R.* c. *Spencer*, préc., note 94, par. 32.
[100] *R.* c. *Marakah*, préc., note 81, par. 21.
[101] *R.* c. *Cole*, préc., note 94, par. 51; *R.* c. *Buhay*, préc., note 50, par. 22; *Hunter* c. *Southam inc.*, préc., note 4, 158.

Par ailleurs, comme le note Steve Coughlan[102], ce facteur est parfois aussi présenté sous la question de la qualité pour agir (*standing*). Ce fut notamment le cas dans la dissidence du juge Moldaver dans *Marakah*[103]. Dans tous les cas, ce critère doit être considéré.

C) L'existence d'une attente subjective

La reconnaissance d'une attente subjective ne doit pas être un critère exigeant à remplir[104]. À cette étape, on ne se soucie pas du caractère raisonnable de cette attente subjective, mais seulement de son existence. Celle-ci peut être établie à l'aide de témoignage, mais également par présomption[105].

D) Le caractère raisonnable de cette attente subjective, eu égard à l'ensemble des circonstances

Finalement, lorsqu'il s'agit de déterminer si l'attente de vie privée de l'individu est raisonnable, les critères de l'arrêt *Edwards* énoncés ci-dessus peuvent être utilisés, de même que ceux établis dans *Patrick* et *Tessling* également susmentionnés. Ces critères varieront nécessairement selon la sphère de vie privée pertinente. Toutefois, selon la Cour dans *Marakah*, certains facteurs sont plus utilisés que les autres, soient les facteurs du lieu fouillé, du caractère privé de l'objet de la fouille et du contrôle du demandeur sur l'objet de la fouille[106].

Bien évidemment, le facteur du lieu de la fouille est appelé à être modifié dans un contexte de fouilles technologiques, mais nous y reviendrons. Dans un contexte de fouilles plus « traditionnelles » toutefois, ce facteur revêt nécessairement une importance accrue. En effet, la résidence est habituellement l'endroit où un individu aura la plus grande attente de vie privée, « [i]l n'existe aucun endroit au monde où une personne possède une attente plus grande en matière de vie privée que dans sa "maison d'habitation" »[107]. Ce constat a d'ailleurs été jugé

---

[102] S. G. COUGHLAN, préc., note 3, p. 79.
[103] *R.* c. *Marakah*, préc., note 81, par. 102 et suivants.
[104] P. BÉLIVEAU et M. VAUCLAIR, préc., note 41, par. 860.
[105] *R.* c. *Patrick*, préc., note 44, par. 37.
[106] *R.* c. *Marakah*, préc., note 81, par. 24.
[107] *R.* c. *Feeney*, préc., note 45, par. 43.

conforme au principe que l'article 8 de la *Charte* protège « les personnes et non les lieux »[108], puisqu'il s'agit alors de vérifier le caractère raisonnable de l'attente de vie privée d'un individu[109].

Tel que mentionné ci-dessus, ce qui est susceptible d'être révélé sur un individu par la technique d'enquête doit être considéré lors de la détermination de l'objet d'une fouille. Or, ces considérations sont également pertinentes lorsqu'il s'agit de déterminer du caractère raisonnable d'une attente subjective de vie privée. Autrement dit, « le risque de divulgation de renseignements privés est un facteur dont il faut tenir compte pour décider si une conversation électronique suscite des attentes raisonnables en matière de respect de la vie privée et est protégée par l'art. 8 de la *Charte* »[110]. Bien qu'énoncé par la Cour dans un contexte de conversation électronique par messagerie texte, cela vaut également pour toute fouille visant des renseignements d'ordre biographique. De plus, le caractère privé de l'information dévoilée par la technique d'enquête est pertinent, et ce, même si les renseignements protégés sont de nature criminelle[111].

Selon la Cour suprême, trois facettes se chevauchent lorsqu'il est question d'examiner le caractère privé des renseignements personnels, soit la confidentialité, le contrôle et l'anonymat[112]. La confidentialité sera une considération importante surtout lorsqu'il s'agira de relation entre un individu et un professionnel, tel qu'un avocat ou un médecin. L'anonymat, pour sa part, peut avoir plusieurs applications, mais sera particulièrement important lorsqu'il est question de l'utilisation d'Internet. La Cour suprême a effectivement reconnu que plusieurs individus utilisent l'Internet de façon anonyme, notamment en raison de la quantité importante de renseignements pouvant être recueillies lors de l'utilisation d'Internet, et que « [l]'anonymat pourrait donc, compte tenu de l'ensemble des circonstances, servir de fondement au droit à la vie privée »[113]. La notion de contrôle, bien qu'étudiée dans le cadre du facteur du caractère privé

---

[108] *Hunter* c. *Southam inc.*, préc., note 4, 159.
[109] *R.* c. *Tessling*, préc., note 2, par. 22.
[110] *R.* c. *Marakah*, préc., note 81, par. 31.
[111] *R.* c. *Spencer*, préc., note 94, par. 36.
[112] *Id.*, par. 39.
[113] *Id.*, par. 48.

des renseignements dans la décision *Spencer*, mérite une analyse séparée, notamment en raison de l'importance qui lui est accordée dans *Marakah*.

La notion de contrôle est en effet au cœur du désaccord entre la majorité et le juge Moldaver dans *Marakah*. Il est toutefois possible de dégager certains principes qui font l'unanimité. D'abord, il importe de rappeler que le contrôle n'est qu'un élément parmi tant d'autres qui peuvent être pertinents à cette étape de l'analyse[114]. La notion de contrôle renvoie au droit que possède un individu de décider quand, comment et dans quelle mesure les informations qu'il possède seront divulguées[115]. Cela inclut également le droit de ne pas divulguer ces renseignements[116].

Le fait que le contrôle d'un bien soit partagé n'annihile pas nécessairement la possibilité qu'une attente raisonnable de vie privée existe[117]. Cette conclusion est directement en lien avec le rejet de l'analyse fondée sur le risque dans la décision *Duarte*. Dans un même ordre d'idées, le contrôle n'est pas synonyme de propriété[118]. Ainsi, il est possible d'exercer un contrôle sur un objet ou des renseignements qui appartiennent véritablement à un tiers[119]. Bref, comme toujours, une analyse contextuelle s'impose lorsqu'il s'agit de déterminer si un individu peut prétendre avoir le contrôle sur un renseignement, un bien ou un lieu.

E) L'importance du contexte normatif

Par ailleurs, il importe de remarquer que, bien que l'approche soit contextuelle, elle n'est pas purement factuelle[120]. Le contexte normatif est également pertinent afin de déterminer s'il y a présence d'une attente raisonnable de vie privée[121]. Cela veut dire que certaines normes ou

---

[114] Le juge Moldaver, bien que d'avis qu'un certain contrôle est généralement nécessaire à l'établissement d'une attente raisonnable de vie privée, reconnaît tout de même que le contrôle n'est pas nécessaire, dans certaines situations exceptionnelles. *R.* c. *Marakah*, préc., note 81, par. 130.
[115] *R.* c. *Spencer*, préc., note 94, par. 40.
[116] *R.* c. *Dyment*, préc., note 27, 429.
[117] *R.* c. *Cole*, préc., note 94, par. 58; *R.* c. *Gomboc*, préc., note 24, par. 41; *R.* c. *Marakah*, préc., note 81, par. 41; *Id.*, 133, dans la dissidence du juge Moldaver.
[118] Voir notamment la dissidence dans *R.* c. *Marakah*, préc., note 81, par. 118.
[119] *Id.*, par. 43.
[120] *R.* c. *Spencer*, préc., note 94, par. 18.
[121] *Id.*

conventions sociales doivent également être considérées lors de la détermination de l'existence d'une attente raisonnable de vie privée[122]. L'arrêt *Wong* serait l'apogée de cette approche selon un auteur[123], en raison notamment de la référence au roman *1984* de George Orwell[124], mais il importe de remarquer que plusieurs décisions de la Cour suprême ont également traité de l'importance de respecter certaines conventions sociales préétablies[125]. Cette conclusion amène également une tangente : si les conventions sociales changent, l'analyse en vertu de l'article 8 de la *Charte* peut également changer[126].

Section 1.2 Les fouilles, saisies ou perquisitions effectuées sans autorisation judiciaire préalable

Il ne fait pas partie du cadre de ce mémoire que d'étudier toutes les situations où une fouille, saisie ou perquisition peut avoir lieu sans l'obtention préalable d'une autorisation judiciaire. Toutefois, certains cas plus fréquents méritent d'être soulignés, comme le cas de fouille accessoire à une détention ou à une arrestation légale, les cas d'urgence, les cas où un consentement est obtenu et le cas des « objets bien en vue » (connu plus généralement comme la théorie du *plain view*). Par ailleurs, lorsque viendra le temps d'étudier la fouille des ordinateurs, ces principes pourront trouver application dans certaines situations précises.

1.2.1 La fouille accessoire à une arrestation

Le pouvoir de fouille accessoire à une arrestation a été examiné en détail pour la première fois par la Cour suprême en 1990 dans la décision *Cloutier c. Langlois*[127]. Sous la plume de

---

[122] Selon L. M. AUSTIN, préc., note 73, il importe de considérer le contexte normatif afin d'éviter de tomber dans une analyse purement descriptive des attentes des individus, par opposition à une analyse fondée sur la vie privée des gens.
[123] J. A. Q. STRINGHAM, préc., note 73.
[124] *R.* c. *Wong*, préc., note 1, 47.
[125] *R.* c. *Buhay*, préc., note 50, par. 21; *R.* c. *Gomboc*, préc., note 24, par. 34; *R.* c. *Wise*, [1992] 1 R.C.S. 527, 534; *R.* c. *Tessling*, préc., note 2, par. 42.
[126] J. A. Q. STRINGHAM, préc., note 73.
[127] *Cloutier* c. *Langlois*, [1990] 1 R.C.S. 158. Ce principe avait été seulement soulevé de manière sommaire auparavant, dans les décisions *R.* c. *Debot*, [1989] 2 R.C.S. 1140; *R.* c. *Beare*, [1988] 2 R.C.S. 387.

l'honorable juge L'Heureux-Dubé, la Cour conclut à l'existence d'un pouvoir de *common law* autorisant les policiers, selon certaines conditions, à fouiller un individu lors de son arrestation :

> « […] il me semble indubitable que la *common law* telle qu'elle a été reçue et a évolué au Canada reconnaît aux policiers le pouvoir de fouiller la personne légalement mise en état d'arrestation et de saisir les objets en sa possession ou dans son entourage immédiat dans le but d'assurer la sécurité des policiers et du prévenu, d'empêcher l'évasion du prisonnier ou encore de constituer une preuve contre ce dernier »[128].

Ce pouvoir – qui n'impose par ailleurs aucun devoir aux policiers[129] – a depuis été précisé et raffiné par de nombreuses décisions judiciaires. D'abord, il est utile de rappeler que trois conditions doivent être satisfaites pour qu'une fouille soit véritablement effectuée en vertu de ce pouvoir : premièrement, l'arrestation doit être légale[130], deuxièmement la fouille doit être véritablement accessoire à l'arrestation et troisièmement, la fouille doit avoir été effectuée de manière raisonnable[131]. Ce pouvoir ne découle pas de l'urgence de la situation, « mais sur l'existence d'un lien ou d'un rapport avec l'infraction pour laquelle le suspect a été arrêté »[132].

Afin que la seconde condition soit respectée, « les policiers doivent tenter de réaliser un objectif valable lié à l'arrestation »[133]. À ce niveau, il n'est pas nécessaire que les policiers aient eu des motifs raisonnables et probables de procéder à la fouille accessoire, mais seulement qu'ils pensaient raisonnablement que celle-ci était justifiée (critère subjectif et objectif). Les policiers ont donc une « marge de manœuvre considérable »[134] dans ce cas. Par ailleurs, lorsque les policiers utilisent ce pouvoir de fouille afin de rechercher d'autres éléments de preuve, ils doivent limiter leurs recherches à des éléments en lien avec l'infraction qui est présentement sous enquête[135]. Une certaine limite temporelle s'applique également, quoique celle-ci peut varier selon les circonstances[136].

---

[128] *Cloutier* c. *Langlois*, préc., note 128, 180-181.
[129] *Id.*, 186.
[130] Selon les paramètres établis à la partie XVI du *Code criminel* ou en vertu d'une autre loi.
[131] *R.* c. *Stillman*, préc., note 49, par. 27.
[132] *R.* c. *Fearon*, [2014] 3 R.C.S. 621, par. 25; reprenant *R.* c. *Nolet*, [2010] 1 R.C.S. 851, par. 52.
[133] *R.* c. *Caslake*, [1998] 1 R.C.S. 51, par. 19.
[134] *Id.*, par. 20.
[135] *Id.*, par. 22.
[136] *Id.*, par. 24.

Ce pouvoir inclut le droit de fouiller l'environnement où a eu lieu l'arrestation, de même qu'un véhicule se trouvant à proximité[137]. Il peut également inclure, tel que mentionné, une fouille à nu, mais certaines conditions précises s'ajoutent alors[138]. Toutefois, ce pouvoir n'inclut pas le prélèvement d'échantillons de substances corporelles[139], ni le pouvoir d'effectuer une fouille pour inventaire d'un lieu ayant déjà fait l'objet d'une fouille, quoique la tenue d'une telle fouille n'est généralement pas fatale en ce qui concerne l'exclusion des éléments de preuve, en vertu de l'article 24(2) de la *Charte*[140].

Par ailleurs, en ce qui concerne spécifiquement les cellulaires, qui sont assimilés à des ordinateurs lorsqu'ils disposent de capacité de stockage de données importantes[141], leur fouille est possible de manière accessoire à une arrestation. En effet, selon la Cour suprême dans l'arrêt *Fearon*, il est possible que la fouille d'un cellulaire soit accessoire à une arrestation, dans certains cas précis[142]. Ainsi, les policiers pourront accéder au contenu du cellulaire d'une personne se trouvant en état d'arrestation, et ce, sans obtenir de mandat de perquisition.

Afin que la fouille d'un cellulaire effectuée de manière accessoire à une arrestation soit conforme avec l'article 8 de la *Charte*, certaines conditions additionnelles doivent être respectées. Ces conditions découlent du fait que les cellulaires, tout comme les ordinateurs :

> « […] peuvent avoir une immense capacité de stockage, peuvent générer des données concernant la vie intime de l'utilisateur, comme ses intérêts, ses habitudes et son identité; ils peuvent conserver à l'insu de l'utilisateur ou sans son intention des données même lorsque l'utilisateur croit les avoir supprimées, et peuvent donner accès à des renseignements qui ne se trouvent pas concrètement "à l'endroit" où la fouille est effectuée. »[143]

---

[137] *R.* c. *Stillman*, préc., note 49, par. 48.
[138] *R.* c. *Golden*, préc., note 4.
[139] *R.* c. *Stillman*, préc., note 49, par. 49.
[140] *R.* c. *Nolet*, préc., note 133, par. 53-54.
[141] *R.* c. *Vu*, [2013] 3 R.C.S. 657, par. 38; *R.* c. *Fearon*, préc., note 133, par. 54.
[142] *R.* c. *Fearon*, préc., note 133.
[143] *Id.*, par. 51; reprenant les propos tenus dans *R.* c. *Vu*, préc., note 142, par. 41-44.

Ainsi, les policiers devront s'assurer de respecter des conditions additionnelles afin de balancer le droit à la vie privée des individus et les objectifs importants d'application de la loi qui peuvent être réalisés lors de la fouille de cellulaires[144]. Tel que le présente la Cour :

> « En résumé, les policiers ne seront pas autorisés à procéder à la fouille d'un téléphone cellulaire ou d'un appareil similaire accessoirement à chaque arrestation. Les fouilles de cette nature seront plutôt conformes à l'art. 8 lorsque :
>
> (1) l'arrestation est légale;
>
> (2) la fouille est véritablement accessoire à l'arrestation puisque les policiers peuvent invoquer un objectif d'application de la loi valable et objectivement raisonnable pour procéder à la fouille; dans ce contexte, les objectifs valables d'application de la loi sont les suivants :
>
> a) protéger les policiers, l'accusé ou le public;
>
> b) conserver les éléments de preuve;
>
> c) découvrir des éléments de preuve, notamment trouver d'autres suspects, lorsque l'enquête sera paralysée ou sérieusement entravée si l'on n'effectue pas rapidement une fouille accessoire à l'arrestation à l'égard du téléphone cellulaire;
>
> (3) la nature et l'étendue de la fouille sont adaptées à l'objectif de la fouille;
>
> (4) les policiers prennent des notes détaillées de ce qu'ils ont examiné dans l'appareil et de la façon dont ils l'ont fait. »[145]

À la troisième étape, il importe de souligner que ce n'est pas l'entièreté du cellulaire qui pourra être fouillée, mais seulement les données directement en lien avec les objectifs justifiant la fouille. Ainsi, de manière générale « seuls les courriels envoyés ou rédigés récemment, les photos et messages texte récents, ainsi que le registre des appels, pourront être examinés »[146]. Par ailleurs, ce seront généralement des infractions comportant des éléments de violence ou qui présentent une menace à la sécurité du public qui justifieront le recours à la fouille d'un

---

[144] *R.* c. *Fearon*, préc., note 133, par. 49.
[145] *Id.*, par. 83.
[146] *Id.*, par. 76.

téléphone cellulaire de manière incidente à une arrestation[147]. Il importe aussi de souligner que l'objectif de recherche de nouveaux éléments de preuve ne pourra justifier une fouille incidente d'un cellulaire seulement lorsque l'enquête risque d'être sérieusement entravée à défaut de cette fouille[148].

La décision *Fearon* a été largement critiquée par les organisations militant pour les libertés civiles[149], mais également par certains auteurs qui soulignent l'incohérence de la décision par rapport au corpus de la Cour suprême en matière de fouille incidente à une arrestation[150] et également le fait que la décision fasse primer l'application efficace de la loi sur la vie privée des citoyens[151].

1.2.2 La fouille accessoire à une détention aux fins d'enquête et la fouille pour motifs de sécurité

L'existence d'un pouvoir de *common law* autorisant la détention d'un individu à des fins d'enquête a été confirmée dans la décision *Mann* en 2004[152]. Tel que souligné dans la décision, ce pouvoir de *common law* a été largement utilisé au Canada avant que la Cour suprême ne se penche sur cette question[153].

La détention ne vise pas toutes les situations où les policiers ont un contact avec un individu. Pour que le terme détention s'applique, il devra y avoir une contrainte psychologique ou physique appréciable, de la part des policiers sur l'individu en question[154]. Afin que les policiers

---

[147] *Id.*, par. 79.
[148] *Id.*, par. 80.
[149] Kassie SEABY et Raji MANGAT, « Making Privacy Meaningful in a Digital Age », *British Columbia Civil Liberties Association* (15 décembre 2014), en ligne : BCCLA <https://bccla.org/2014/12/making-privacy-meaningful-in-a-digital-age/> (consulté le 9 avril 2018).
[150] Agathon FRIC, « Reasonableness as Proportinality: Towards a Better Constructive Interpretation of the Law on Searching Computers in Canada », (2016) 21 *Appeal Rev. Curr. Law Law Reform CA* 59.
[151] Nader R. HASAN, « A Step Forward of Just a Sidestep? Year Five of the Supreme Court of Canada in the Digital Age », (2015) 71 *Supreme Court Law Rev.* 439.
[152] *R.* c. *Mann*, préc., note 4.
[153] *Id.*, par. 16 citant A. YOUNG, « All Along the Watchtower: Arbitrary Detention and the Police Function » (1991), 29 *Osgoode Hall L.J.* 329, p. 330; et J. STRIBOPOULOS, « A Failed Experiment? Investigative Detention: Ten Years Later » (2003), 41 *Alta. L. Rev.* 335, p. 339.
[154] *Id.*, par. 19.

puissent détenir quelqu'un aux fins d'enquête, ils devront avoir des motifs raisonnables de soupçonner que cet individu est impliqué dans la commission d'une infraction[155]. Autrement dit :

> « La détention doit être jugée raisonnablement nécessaire suivant une considération objective de l'ensemble des circonstances qui sont à la base de la conviction du policier qu'il existe un lien clair entre l'individu qui sera détenu et une infraction criminelle récente ou en cours. »[156]

Lorsque les policiers détiennent un individu en vertu de ce pouvoir, ils auront également la possibilité de fouiller cet individu. Toutefois, il importe de souligner que ce pouvoir n'est pas aussi vaste que celui de procéder à une fouille accessoire à une arrestation. Ainsi, les policiers pourront effectuer une fouille accessoire à une détention, seulement s'ils ont des motifs raisonnables de craindre pour leur propre sécurité ou celle du public[157]. Ce pouvoir de fouille pour des motifs de sécurité n'existe donc pas de manière autonome[158], contrairement au pouvoir de fouille accessoire à une arrestation qui ne nécessite pas que les policiers aient des motifs raisonnables de croire à la nécessité d'une telle fouille[159]. Cette fouille sera limitée à une fouille par palpation, qui est peu intrusive et qui permet d'assurer la sécurité des policiers et du public.

Par ailleurs, dans la décision *MacDonald*[160], la Cour s'est fondée sur la décision *Mann* afin de créer un pouvoir de fouille pour des motifs de sécurité, qui existe indépendamment d'une arrestation ou d'une détention. Selon cette décision, les policiers pourront effectuer une fouille pour des motifs de sécurité lorsque celle-ci est « raisonnablement nécessaire pour éliminer une menace imminente à leur sécurité ou à celle du public »[161] et qu'ils ont des motifs raisonnables

---

[155] *Id.*, par. 34.
[156] *Id.*
[157] *Id.*, par. 40.
[158] *Id.*
[159] Pour cette raison, certains auteurs soutiennent que l'expression « fouille incidente à une détention » n'est pas appropriée. Voir S. G. COUGHLAN, préc., note 3, p. 103.
[160] *R.* c. *MacDonald*, préc., note 23.
[161] *Id.*, par. 40.

de croire que leur sécurité ou celle du public est en danger[162]. La fouille sera alors limitée à la recherche d'armes[163].

Selon les conditions afférentes à ces deux pouvoirs de fouille, il est clair que ceux-ci ne pourront permettre aux policiers de saisir des appareils électroniques qui seraient découverts sur les individus visés par la fouille. Néanmoins, nous jugeons utile de traiter de ces deux pouvoirs dans le cadre de ce mémoire afin de présenter adéquatement les pouvoirs de fouille les plus couramment utilisés au Canada. Par ailleurs, ces pouvoirs de fouille – qui peuvent constituer une première approche avec un suspect – peuvent ensuite justifier une arrestation, ce qui permettrait alors une fouille incidente à une arrestation lors de laquelle un cellulaire pourrait être saisi, ou l'obtention d'un mandat de perquisition.

1.2.3 La fouille en cas d'urgence

Bien que l'obtention préalable d'un mandat de perquisition soit la norme, l'urgence de la situation peut parfois permettre aux policiers d'effectuer une fouille sans autorisation judiciaire[164]. Selon la décision *Grant*, les policiers pourront effectuer une fouille ou une perquisition sans mandat dans un endroit autre qu'une maison d'habitation, mais seulement « s'il existe un risque imminent que les éléments de preuve recherchés […] soient perdus, enlevés, détruits ou qu'ils disparaissent si la fouille, la perquisition ou la saisie est retardée aux fins de l'obtention d'un mandat. »[165] La décision *Silveira* confirme que ce pouvoir ne peut être utilisé afin d'effectuer une perquisition dans une maison d'habitation[166].

Toutefois, même lorsqu'un tel risque existe, les policiers devront tout de même respecter les critères permettant l'octroi d'un mandat. En d'autres mots, « exigent circumstances do not justify a warrantless search for evidence or contraband on less than grounds for obtaining a warrant. »[167] Cette doctrine permet donc aux policiers de contourner l'exigence d'obtenir une

---

[162] *Id.*, par. 41.
[163] *Id.*, par. 39; S. G. COUGHLAN, préc., note 3, p. 103.
[164] En anglais, ce type de fouille est désigné sous les termes « *exigent circumstances* ».
[165] *R.* c. *Grant*, [1993] 3 R.C.S. 223, 241-242; Voir aussi *R.* c. *Colarusso*, préc., note 87, 53.
[166] *R.* c. *Silveira*, [1995] 2 R.C.S. 297, par. 50-52.
[167] *R.* v. *Kelsy*, 2011 ONCA 605, par. 25.

autorisation judiciaire en raison des conséquences que pourraient avoir les délais entourant l'obtention de ladite autorisation, non pas parce qu'ils ne remplissent pas les critères permettant d'obtenir celle-ci.

Par ailleurs, il est important de noter que la détermination de l'urgence de la situation doit se faire au cas par cas[168]. Il n'existe donc pas de catégorie générale, telle que la preuve se trouvant à bord d'une voiture par exemple[169], permettant de contourner l'exigence d'obtenir un mandat de perquisition.

1.2.4 La fouille avec consentement

Évidemment, l'individu jouissant de l'attente de vie privée a toujours le loisir de renoncer à la protection qui lui est offerte par la *Charte*[170]. Il appartiendra alors au ministère public de prouver que l'individu a donné un consentement libre et éclairé[171]. Par ailleurs, pour qu'un consentement soit valide, l'individu « doit être en mesure d'empêcher la police d'effectuer la fouille, perquisition ou saisie en refusant de le donner »[172]. Il faut également que l'individu comprenne les conséquences de sa renonciation à invoquer la protection de la *Charte*[173]. L'individu devra donc avoir accès à « tous les renseignements requis pour pouvoir renoncer réellement à ce droit »[174], ce qui inclut de savoir si la preuve ainsi recueillie peut être utilisée pour plus d'une enquête déjà en cours[175].

Il est donc théoriquement possible que les policiers obtiennent des appareils électroniques d'un suspect en lui demandant de consentir à la saisie. Toutefois, il est bien évident que cette

---

[168] S. G. COUGHLAN, préc., note 3, p. 106.
[169] *R.* c. *Grant*, préc., note 166, 242.
[170] Bien évidemment, seule la personne possédant l'attente de vie privée peut fournir un consentement valide à une fouille. *R.* c. *Cole*, préc., note 94, par. 79.
[171] *R.* c. *Mellenthin*, 1992 3 R.C.S. 615, 624 *in fine*.
[172] *R.* c. *Stillman*, préc., note 49, par. 60.
[173] P. BÉLIVEAU et M. VAUCLAIR, préc., note 41, par. 877, citant *R.* c. *Wills* (1992), 70 C.C.C. (3d) 529 (C.A.O.).
[174] *R.* c. *Borden*, préc., note 28, 162.
[175] *Id.*, 164. Ceci n'interdit toutefois pas la conservation des éléments de preuve pour des enquêtes futures non encore connues des policiers. Voir *R.* c. *Arp*, [1998] 3 R.C.S. 339.

technique sera rarement – voir jamais – utilisée en raison du risque que l'individu refuse et détruise ensuite les données se trouvant dans les appareils.

1.2.5 La théorie des « objets bien en vue » (théorie du **plain view***)*

La théorie des « objets bien en vue », plus souvent connue sous le vocable anglophone de théorie du *plain view*, revêt une importance particulière lorsqu'il est question de la fouille d'un ordinateur. Cette application particulière de la théorie sera examinée plus amplement ci-dessous, à la section 2.4 du présent mémoire. Pour le moment, nous examinerons les bases de cette théorie, telles qu'élaborées par la *common law*.

La théorie des « objets bien en vue » appliquée en droit criminel canadien provient de la jurisprudence américaine[176]. Pour que la théorie s'applique et que les policiers se soustraient ainsi à l'obligation d'obtenir un mandat visant précisément les objets qu'ils s'apprêtent à saisir, trois conditions doivent être respectées :

> « (i) the seizing officer must be lawfully in the place of seizure; (ii) the evidentiary nature of the item must be immediately apparent to the officer through the unaided use of his or her senses; and (iii) the evidence must be discovered inadvertently. »[177]

Ainsi, les policiers doivent se trouver légalement sur les lieux où se trouvent les objets[178]. Cela pourrait évidemment être lors de l'exécution d'un mandat de perquisition spécifiant d'autres objets[179], mais également lors de l'interception d'un véhicule en vertu du *Code de la sécurité routière*[180], lors d'une entrée dans une résidence à la suite d'un appel aux services d'urgence[181] ou lors d'une arrestation avec mandat dans une résidence[182]. Par ailleurs, un policier ne pourrait saisir un document qui, à première vue et selon les compétences du policier, n'est pas

---

[176] Lisa JORGENSEN, « In Plain View: R v Jones and the Challenge of Protecting Privacy Rights in an Era of Computer Search », (2013) 46 *UBC Rev* 791, par. 14.
[177] *R.* v. *Atkinson*, 2012 ONCA 380, par. 57.
[178] *R.* c. *Buhay*, préc., note 50, par. 37.
[179] Voir notamment *R.* v. *Middleton*, 2000 BCCA 660.
[180] *R.* c. *Guérin*, 2011 QCCQ 57, par. 18-20; *R.* c. *Lenneville*, 2007 QCCA 400.
[181] *R.* c. *Maheux*, 2016 QCCQ 19690.
[182] *R.* c. *Desjardins*, 2014 QCCS 6695, par. 81-82.

incriminant à sa face même[183]. Toutefois, un policier peut tout de même manipuler l'objet afin d'en découvrir le caractère illégal[184].

Une controverse jurisprudentielle existe quant à la question de savoir si la théorie des « objets bien en vue » a été codifiée à l'article 489 C.cr. Selon cette disposition, un policier peut saisir des objets non spécifiés au mandat lorsqu'il croit, pour des motifs raisonnables, que les objets sont liés à une infraction ou qu'ils pourraient servir de preuve concernant la perpétration d'une infraction. D'un côté, certaines décisions et certains auteurs affirment qu'il s'agit essentiellement d'une codification de la théorie de *common law*[185], tandis que d'autres décisions sont à l'effet contraire[186]. Quoique l'article 489 C.cr. semble effectivement avoir des conditions moins exigeantes que la théorie des « objets bien en vue », il n'en demeure pas moins que ces deux sources distinctes permettent d'arriver au même résultat, soit la saisie d'éléments de preuve qui ne sont pas expressément mentionnés au mandat de perquisition[187].

Section 1.3 Les autorisations judiciaires prévues au *Code criminel*

Puisque nous tenterons ultimement de déterminer quel type d'ordonnance judiciaire sera nécessaire pour que les policiers puissent effectuer des saisies de données sauvegardées dans le *nuage*, il appert nécessaire de se pencher sur les différentes ordonnances prévues au *Code criminel* ainsi que leurs conditions d'application respectives.

Il importe en revanche de souligner que nous ne procéderons pas à une analyse exhaustive du processus d'émission des différentes autorisations judiciaire prévues au *Code criminel*. Ainsi, les questions reliées à la suffisance des motifs présentés par les policiers au juge émetteur ne

---

[183] *R.* c. *Law*, [2002] 1 R.C.S. 227, par. 27.
[184] *R.* c. *2952-1366 Québec inc.*, 2000 CanLII 10009 (QC CA), par. 14.
[185] *R.* c. *Boudreau-Fontaine*, 2010 QCCA 1108, par. 50; *R.* v. *Witen*, 2010 ONSC 388, par. 19; Voir aussi P. BÉLIVEAU et M. VAUCLAIR, préc., note 41, par. 949.
[186] *R.* c. *Bottineau*, 2011 ONCA 194; *R.* v. *Frieburg (T.L.)*, 2013 MBCA 40; *R.* v. *Sipes*, 2011 BCSC 1763, par. 213.
[187] Voir *R.* c. *Desjardins*, préc., note 183, par. 81 qui résume bien la controverse entourant cette disposition et qui conclut essentiellement qu'une saisie peut être autorisée par la *common law* ou l'article 489 C.cr., sans différence majeure.

seront pas étudiées. De même, nous n'étudierons pas les considérations relatives à la révision des mandats.

1.3.1 Le mandat de perquisition

Lorsque les policiers veulent effectuer une perquisition dans un lieu spécifique, tels qu'une maison, un appartement ou une place d'affaires, le mandat de perquisition prévu à l'article 487 C.cr. sera utilisé. Cette disposition permet à un juge d'émettre un mandat visant un bâtiment, contenant ou lieu s'il existe des motifs raisonnables de croire qu'on peut y trouver soit :

> « **a)** une chose à l'égard de laquelle une infraction à la présente loi, ou à toute autre loi fédérale, a été commise ou est présumée avoir été commise;
>
> **b)** une chose dont on a des motifs raisonnables de croire qu'elle fournira une preuve touchant la commission d'une infraction ou révélera l'endroit où se trouve la personne qui est présumée avoir commis une infraction à la présente loi, ou à toute autre loi fédérale;
>
> **c)** une chose dont on a des motifs raisonnables de croire qu'elle est destinée à servir aux fins de la perpétration d'une infraction contre la personne, pour laquelle un individu peut être arrêté sans mandat;
>
> **c.1)** un bien infractionnel, »[188]

Il est donc important que le mandat précise les objets qui feront l'objet de la perquisition, sans quoi celui-ci peut être invalidé. Par ailleurs, les objets pouvant être visés par le mandat peuvent être variés, considérant que l'expression « preuve touchant la commission d'une infraction », prévue au sous-alinéa 487(1)b) C.cr., a été interprétée de manière à inclure « tous les éléments de preuve qui pourraient jeter la lumière sur les circonstances d'un événement qui paraît constituer une infraction »[189].

De manière générale, le mandat de perquisition de l'article 487 C.cr. permet aux policiers de fouiller tout ce qui se trouve dans le lieu, du moment où les choses précisées au mandat peuvent

---

[188] *Code criminel*, préc., note 17, art. 487.
[189] *CanadianOxy Chemicals Ltd.* c. *Canada (Procureur général)*, [1999] 1 R.C.S. 743, par. 15.

s'y trouver[190]. Par exemple, si des documents sont mentionnés au mandat de perquisition, les policiers pourront ouvrir des tiroirs, des armoires et des contenants afin de localiser lesdits documents. Selon la Cour suprême, « [c]ette règle générale repose sur l'hypothèse selon laquelle, si l'exécution d'une perquisition dans un lieu pour y chercher certaines choses est justifiée, la recherche de ces choses dans les contenants découverts dans ce lieu est elle aussi justifiée »[191]. Toutefois, en ce qui concerne les ordinateurs, cette règle générale ne peut s'appliquer, pour des motifs qui seront étudiés en profondeur à la section 2.2 du présent mémoire.

Il importe également de souligner que les sous-paragraphes 487(1)a) et b) C.cr. prévoient que ce mandat de perquisition peut être utilisé afin d'enquêter sur toute infraction à toute loi fédérale[192]. Ainsi, le mandat de perquisition de l'article 487 C.cr. pourra s'appliquer dans une multitude de situations, passant d'infractions en matière de droits d'auteurs aux infractions d'évasion fiscale.

Finalement, le mandat de perquisition ne peut être utilisé afin d'enquêter sur des infractions qui n'ont pas encore été commises[193]. Un autre type d'autorisation judiciaire devra donc être employé pour ce faire.

1.3.2 Le mandat général

L'article 487.01 ne prévoit pas un pouvoir de perquisition en tant que tel. Cet article permet plutôt l'emploi de techniques d'enquête spéciales, qui constitueraient une fouille, saisie ou perquisition abusive, sans une autorisation judiciaire. Ainsi, la disposition peut être utilisée afin d'accomplir une panoplie de gestes, du moment où aucune autre autorisation judiciaire ne

---

[190] *R.* c. *Vu*, préc., note 142, par. 23.
[191] *Id.*, par. 39.
[192] J. A. FONTANA et D. KEESHAN, préc., note 74, p. 52-53.
[193] *R.* v. *Branton*, 2001 CanLII 8535 (ON CA), par. 35. L'utilisation du mandat de l'article 487 C.cr. pour obtenir de la preuve sur des infractions qui n'ont pas encore été commises est parfois désignée comme le « *Branton error* ». Voir notamment *R.* v. *Kramshoj*, 2017 ONSC 2951; *R.* v. *Nurse and Plummer*, 2014 ONSC 1779; *R.* v. *Sonne*, 2012 ONSC 584.

s'applique[194]. Cette condition a pour but que le mandat général ne soit utilisé qu'en dernier recours, sans être utilisé par les forces de l'ordre afin d'éviter de se soumettre à des conditions plus exigeantes qui pourraient s'appliquer aux autres types d'autorisations judiciaires[195]. En plus de cette condition, le juge émetteur doit être convaincu qu'il existe des motifs raisonnables de croire qu'une infraction à une loi fédérale a été ou sera commise et que l'émission du mandat servira au mieux l'administration de la justice.

Cette disposition a été adoptée en 1993, après que l'arrêt *Wong* ait révélé un vide législatif par rapport à l'utilisation de certaines techniques d'enquête, en l'espèce l'utilisation de caméras dans un lieu où une attente de vie privée existe[196]. Selon Steve Coughlan, en adoptant cette disposition le législateur « took a decision that relied on the assumption that there need to be limits to police investigative techniques »[197]. Ainsi, les tribunaux exercent un pouvoir de contrôle *a priori* sur les techniques d'enquête utilisée, plutôt qu'*a posteriori* uniquement.

Cette disposition peut notamment être utilisée afin d'installer des caméras de surveillance dans un lieu précis[198], de prendre des photos des parties intimes d'un accusé qui portaient une marque distinctive permettant à la victime de l'identifier[199], d'effectuer une entrée subreptice d'une résidence[200], d'effectuer des livraisons de drogue contrôlées[201] ou de mettre en scène un vol fictif, afin de saisir de la drogue sans éveiller les soupçons des suspects[202]. Contrairement au mandat de perquisition de l'article 487 C.cr., le mandat général de l'article 487.01 C.cr. peut être utilisé afin d'enquêter sur une infraction qui n'a pas encore été commise[203].

---

[194] *R.* c. *Société TELUS Communications*, [2013] 2 R.C.S. 3, par. 18.
[195] *Id.*, par. 19.
[196] *R.* c. *Wong*, préc., note 1.
[197] S. G. COUGHLAN, préc., note 3, p. 162.
[198] *Code criminel*, préc., note 17, art. 487.01(4).
[199] *R.* c. *H.-G.*, 2005 QCCA 1160.
[200] *Shooner* c. *R.*, 2012 QCCQ 12674.
[201] *R.* v. *Chukwu*, 2016 SKCA 6.
[202] *R.* v. *Knight*, 2008 NLCA 67.
[203] J. A. FONTANA et D. KEESHAN, préc., note 74, p. 486.

Dans un contexte de preuve électronique, cette disposition peut également permettre de faire des copies de données informatiques contenues dans un ordinateur[204]. Nous discuterons également d'autres possibilités d'utiliser cette disposition dans un contexte informatique, à la section 3.3.3 du présent mémoire.

1.3.3 Les ordonnances de communication

De manière générale, les diverses ordonnances de communication prévues au *Code criminel* permettent aux policiers d'obtenir de l'information qui est en la possession ou sous le contrôle d'une tierce partie, souvent une entreprise, qui n'est pas visée par l'enquête. Cette information peut se trouver sous la forme de documents ou encore de données.

Avec le projet de loi C-13 de 2014[205], de nouvelles ordonnances de communication ont été ajoutées au *Code criminel*. Ces ordonnances ne visent pas les mêmes types de documents et n'ont pas nécessairement les mêmes conditions d'application. Nous examinerons donc premièrement l'ordonnance générale de communication, prévue à l'article 487.014 C.cr., avant de nous pencher sur les ordonnances de communication spécifiques, prévues aux articles 487.015 à 487.018 C.cr. Nous survolerons également l'ordre et l'ordonnance de préservations, prévus respectivement aux articles 487.012 et 487.013 C.cr.

Par ailleurs, il est important de spécifier à ce stade que les forces de l'ordre devront utiliser, le cas échéant, l'ordonnance de communication précise qui s'applique à la situation sous étude[206]. En d'autres termes, l'ordonnance générale de communication ne pourra être utilisée si une ordonnance spécifique est disponible. Toutefois, il serait possible d'utiliser une même dénonciation au soutien d'une ordonnance générale et d'une ordonnance spécifique de communication, si les conditions s'appliquant aux différentes ordonnances sont respectées[207].

---

[204] *Keating* v. *Nova Scotia (Attorney General)*, 2001 NSSC 85.
[205] *Loi modifiant le Code criminel, la Loi sur la preuve au Canada, la Loi sur la concurrence et la Loi sur l'entraide juridique en matière criminelle*, projet de loi n°C-13 (sanctionné – 9 décembre 2014), 2e sess., 41e légis. (Can.).
[206] *Alberta (Attorney General)* v. *Provincial Court of Alberta*, 2015 ABQB 728, par. 101.
[207] *Winnipeg Police Service Officer (Re)*, 2015 MBPC 70, par. 23.

1.3.3.1 L'ordonnance générale de communication

L'article 487.014 C.cr. – ou avant les modifications législatives apportées par le projet de loi C-13, l'article 487.012 C.cr. – permet aux policiers d'obtenir une copie de tout document ou donnée qui est en la possession ou à la disposition d'une tierce personne, si le juge émetteur est convaincu qu'il existe de motifs raisonnables de croire à la commission d'une infraction, que les documents et données sont en la possession de cette tierce personne et que celles-ci seront utiles en preuve. Cette disposition ne peut toutefois être utilisée afin d'obtenir de tels documents de la personne visée par l'enquête[208].

Plusieurs types de documents peuvent donc être obtenus en ayant recours à cette disposition. Il pourrait s'agir de documents reliés à un mandat d'aide juridique dans une instance de divorce[209], de matériel audio et vidéo en possession de Radio-Canada[210] ou un autre télédiffuseur[211], de documents détenus par un ombudsman provincial[212], de dossiers médicaux[213], etc.

Dans la décision *Spencer*, qui constitue l'élément déclencheur ayant mené à l'adoption du projet de loi C-13, la Cour suprême s'est penchée sur la nécessité d'obtenir une ordonnance de communication afin d'obtenir les renseignements relatifs à l'abonné lié à une adresse IP précise, ayant servi à télécharger de la pornographie juvénile. Considérant que l'accusé avait une attente raisonnable de vie privée à l'égard de son identité virtuelle, qui correspond à une activité informatique particulière[214], la Cour a conclu que les policiers auraient dû obtenir une ordonnance de communication afin d'obtenir une copie de ces documents[215].

Par ailleurs, selon la Cour provinciale de l'Alberta, les nouvelles dispositions créées par le projet de loi C-13 ne modifient en rien la conclusion de la Cour suprême dans l'arrêt *Spencer* à l'effet

---

[208] *Code criminel*, préc., note 17, art. 487.014(4).
[209] *Directeur des poursuites criminelles et pénales du Québec* c. *Nicolo*, 2016 QCCS 3419.
[210] *R.* c. *Trudeau*, 2016 QCCQ 925.
[211] *Global TV* v. *Alberta*, 2013 ABPC 342.
[212] *R.* v. *Nova Scotia (Ombudsman)*, 2016 NSSC 273.
[213] *R.* c. *Stevenson George Alles*, 2014 QCCQ 12000.
[214] *R.* c. *Spencer*, préc., note 94, par. 33.
[215] *Id.*, par. 49.

qu'une ordonnance générale de communication est nécessaire afin d'obtenir cette information, c'est-à-dire les renseignements relatifs à un abonné[216]. Selon la Cour, la définition des termes « données de transmission » et « données de localisation », prévues à l'article 487.011 C.cr., ne peut inclure les renseignements relatifs à un abonné[217]. Ainsi, les policiers devraient encore se prémunir d'une ordonnance générale de communication, avec son standard des motifs raisonnables de croire à la commission d'une infraction, plutôt qu'une ordonnance de communication spécifique, qui prévoit au contraire un standard plus faible, soit celui des motifs raisonnables de soupçonner la commission d'une infraction.

1.3.3.2 Les ordonnances de communication spécifiques

Le *Code criminel* prévoit quatre ordonnances de communication spécifiques, soit l'ordonnance de communication en vue de retracer une communication spécifique (art. 487.015 C.cr.), l'ordonnance de communication pour des données de transmission (art. 487.016 C.cr.)[218], l'ordonnance de communication pour des données de localisation (art. 487.017 C.cr.) et l'ordonnance de communication pour des données financières (art. 487.018 C.cr.). Les dispositions visant les données de transmission et les données de localisation ont été adoptées avec le projet de loi C-13[219], et ce, notamment afin que le Canada soit en mesure de ratifier la *Convention sur la cybercriminalité* du Conseil de l'Europe dont il est signataire[220].

Le standard d'émission de ces différentes autorisations judiciaires est celui des « motifs raisonnables de soupçonner ». Ainsi, il est plus facile pour les forces de l'ordre d'obtenir de telles autorisations, par opposition à une ordonnance générale de communication.

Dans son mémoire présenté au Sénat du Canada, le Commissaire à la protection de la vie privée Daniel Therrien a énoncé ses craintes par rapport à ce fardeau de preuve plus faible qui est

---

[216] *Re Subscriber Information*, 2015 ABPC 178, par. 35.
[217] *Id.*, par. 36.
[218] Un mandat permettant d'enregistrer de telles données est prévu à l'article 492.2 C.cr.
[219] *Loi modifiant le Code criminel, la Loi sur la preuve au Canada, la Loi sur la concurrence et la Loi sur l'entraide juridique en matière criminelle*, préc., note 205.
[220] *Convention sur la cybercriminalité*, 23 novembre 2001, S.T.E. nº 185 (entrée en vigueur au Canada le 1er novembre 2015).

susceptible de porter atteinte à la vie privée des citoyens canadiens[221]. Or, malgré ces remarques, le projet de loi a été adopté tel quel. Dans ce mémoire, un tableau résumé des différentes ordonnances de communication, comprenant le type de données pouvant être obtenues en vertu de chacune des dispositions ainsi que le seuil d'autorisation prévu, était inclus. Nous avons reproduit celui-ci en *Annexe I*, en raison de sa clarté[222].

Comme ces ordonnances visent spécifiquement les données informatiques, nous étudierons celles-ci en détail à la section 2.2.1.1 du présent mémoire.

1.3.4 L'ordre et l'ordonnance de préservation

De manière connexe, le *Code criminel* prévoit maintenant deux moyens qui permettent aux policiers de s'assurer de la préservation des données informatiques[223] détenues par un tiers, sans toutefois permettre aux policiers de consulter lesdites données.

Dans le cas de l'ordre de préservation, prévu à l'article 487.012 C.cr., un agent de la paix ou un fonctionnaire public peut ordonner à toute personne de préserver des données informatiques qui sont en sa possession ou à sa disposition, et ce, sans autorisation judiciaire émise par un juge. L'agent de la paix ou le fonctionnaire public devra alors être convaincu de l'existence de motifs raisonnables de soupçonner qu'une infraction à une loi fédérale a été ou sera commise, que les données informatiques sont en la possession ou à la disposition de la personne visée par l'ordre et que celles-ci seront utiles à l'enquête. Cet ordre ne peut être donné qu'une seule fois pendant l'enquête et ne peut viser la personne visée par celle-ci.

Pour sa part, l'ordonnance de préservation, prévue à l'article 487.013 C.cr., doit être donnée par un juge. Celui-ci devra s'assurer qu'il existe de motifs raisonnables de soupçonner qu'une

---

[221] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, « Projet de loi C-13, Loi sur la protection des Canadiens contre la cybercriminalité - Mémoire présenté au Comité sénatorial permanent des affaires juridiques et constitutionnelles » (19 novembre 2014), en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/conseils-au-parlement/2014/parl_sub_141119/> (consulté le 17 novembre 2016).

[222] Le tableau contient également les renseignements relatifs aux mandats pour un dispositif de localisation (par. 492.1(1) et (2) C.cr.) dispositions qui ne seront pas étudiées dans le présent mémoire puisque non pertinentes.

[223] Au sens de la définition prévue au paragraphe 342.1(2) C.cr., c'est-à-dire : « représentations, notamment signes, signaux ou symboles, qui sont sous une forme qui en permet le traitement par un ordinateur ».

infraction à une loi fédérale a été ou sera commise, que les données sont en la possession ou à la disposition de la personne visée par l'ordonnance et que celles-ci seront utiles à l'enquête. Il doit également être convaincu que les forces de l'ordre ont l'intention de demander la délivrance d'une autorisation judiciaire afin d'accéder aux données.

Ces dispositions peuvent également être utilisées s'il existe des motifs raisonnables de soupçonner qu'une infraction à la loi d'un État étranger a été commise et que cet État enquête sur cette infraction. Il ne sera toutefois pas possible d'utiliser ces dispositions pour des infractions à une loi étrangère qui n'ont pas encore été commises.

1.3.5 L'interception de communications privées

Le terme « intercepter » est défini à l'article 183 comme le fait « d'écouter, d'enregistrer ou de prendre volontairement connaissance d'une communication ou de sa substance, son sens ou son objet »[224]. Selon la Cour suprême, une interprétation étroite de ce terme est à proscrite, en raison de l'objectif de la partie VI[225]. Ainsi :

> « L'emploi du mot "intercepter" implique que la prise de connaissance de la communication privée se fait au cours du processus de transmission. À mon avis, ce processus englobe toutes les activités du fournisseur de services qui sont nécessaires ou accessoires à la fourniture du service de communication. La prise de connaissance de la substance d'une communication privée se trouvant dans un ordinateur exploité par un fournisseur de services de télécommunications ferait, en conséquence, partie de ce processus. »[226]

Cette interprétation permet de protéger tous les usagers de téléphonie cellulaire, peu importe leur fournisseur. En effet, la Cour dans *TELUS* souligne que cette entreprise est l'une des rares à conserver une copie temporaire des messages envoyés par ses clients sur ses serveurs[227]. L'interprétation restrictive – qui aurait permis aux policiers d'utiliser le mandat général de

---

[224] *Code criminel*, préc., note 17, art. 183.
[225] *R.* c. *Société TELUS Communications*, préc., note 195, par. 35.
[226] *Id.*, par. 37.
[227] *Id.*, par. 7.

l'article 487.01 C.cr. au lieu des dispositions relatives à l'interception des communications privées – aurait donc défavorisé indûment ceux-ci.

L'article 183 définit également l'expression « communications privées », qui doit être faite « dans des circonstances telles que son auteur peut raisonnablement s'attendre à ce qu'elle ne soit pas interceptée par un tiers »[228]. Selon la Cour suprême :

> « […] Si une personne qui peut raisonnablement s'attendre à une certaine intimité, fait, au cours d'une conversation interceptée électroniquement, des déclarations que le ministère public cherche à utiliser contre elle, elle bénéficie, à mon avis, à titre d'auteur de ces déclarations, des dispositions de protection de la vie privée du *Code criminel*, parce que ces déclarations constituent des communications privées de sa part et leur admissibilité à un procès subséquent sera soumise aux dispositions de la Partie IV.1 du *Code criminel.* […] »[229]

Plusieurs types d'autorisations permettent d'intercepter des communications privées. Leur application dépend notamment du consentement d'une partie à la communication. Dans tous les cas, si aucune autorisation ou exception ne s'applique, l'interception sera illégale en vertu de l'article 184 C.cr. Cette disposition rend punissable d'un emprisonnement maximal de cinq ans toute personne qui intercepte de manière illégale des communications privées.

Deux dispositions permettent aux policiers d'intercepter des communications privées sans obtenir d'autorisation judiciaire préalable. Il s'agit des articles 184.1 et 184.4 C.cr. Ces dispositions s'appliquent uniquement lorsqu'un risque de lésions corporelles ou un risque de dommage imminent existe. Dans le cas de l'article 184.4 C.cr., la Cour suprême a conclu à sa validité constitutionnelle, dans la mesure où des mesures de contrôle *a posteriori* additionnelles étaient ajoutées au *Code criminel*[230], ce qui est maintenant le cas aux articles 195 et 196.1[231].

Lorsqu'une des parties à la communication consent à l'interception, l'article 184.2 C.cr. permet à un juge d'une cour provinciale ou supérieure d'émettre une autorisation visant l'interception

---

[228] *Code criminel*, préc., note 17, art. 183.
[229] *Goldman* c. *R.*, [1980] 1 R.C.S. 976, 995.
[230] *R.* c. *Tse*, préc., note 41.
[231] S. G. COUGHLAN, préc., note 3, p. 124.

des communications. Le juge devra alors être convaincu qu'il existe des motifs raisonnables de croire qu'une infraction a été ou sera commise, qu'une des parties à la communication a consenti et que l'interception permettra d'obtenir des renseignements relatifs à l'infraction. Le juge pourra alors inclure dans l'ordonnance toute modalité qu'il estime indiquée dans l'intérêt public.

Toutefois, lorsqu'aucune des parties à la communication ne consent à l'interception, les conditions applicables à l'obtention d'une autorisation d'interception sont plus sévères. D'abord, seul un juge d'une cour supérieure pourra émettre l'autorisation, dont la demande devra être signée par le procureur général de province, par le ministre de la Sécurité publique, ou un représentant désigné par ceux-ci[232]. De plus, le juge devra être convaincu que l'émission de l'autorisation sert au mieux l'administration de la justice et que « d'autres méthodes d'enquête ont été essayées et ont échoué, ou ont peu de chance de succès, ou que l'urgence de l'affaire est telle qu'il ne serait pas pratique de mener l'enquête relative à l'infraction en n'utilisant que les autres méthodes d'enquête »[233]. L'application de ce critère ne doit pas être fondée sur l'efficacité de la technique d'enquête, mais plutôt sur sa nécessité[234].

Traditionnellement, la partie VI du *Code criminel* a été appliquée majoritairement aux communications téléphoniques. Or, qu'en est-il des autres types de communications, par messagerie texte ou via Internet ? Depuis l'arrêt *TELUS*, il est clair que la communication par messagerie texte est visée par les dispositions de la partie VI et qu'une autorisation en vertu de cette partie est donc requise afin d'intercepter des messages textes de manière prospective[235]. Toutefois, si les messages textes sont arrivés à destination et qu'ils sont donc sauvegardés sur un appareil, une telle autorisation n'est pas requise[236]. Un mandat de perquisition visant l'appareil, une ordonnance de communication adressée au FSI ou encore un autre pouvoir de

---

[232] *Code criminel*, préc., note 17, art. 185.
[233] *Id.*
[234] *R.* c. *Araujo*, préc., note 4, par. 21 et suivants.
[235] *R.* c. *Société TELUS Communications*, préc., note 195, par. 12.
[236] *R.* c. *Jones*, préc., note 53, par. 81.

fouille tel que la fouille accessoire à une arrestation[237], serait alors suffisant. Cette approche est toutefois critiquée par certains auteurs[238].

Concernant les communications effectuées sur Internet, par exemple des messages privés envoyés avec une application de type *Facebook, Snapchat* ou *Instagram*, ou encore par *iMessage*, ce service de *Apple* qui ne nécessite pas de forfait de téléphonie cellulaire, mais utilise plutôt l'Internet, nous pensons qu'une application combinée des arrêts *Jones, TELUS* et *Marakah* indique que ceux-ci peuvent faire l'objet d'une attente raisonnable de vie privée. Ainsi, les mêmes principes devraient s'appliquer si les policiers désirent intercepter ou autrement obtenir ce type de conversation.

Section 1.4 La violation de la protection offerte par l'article 8 de la *Charte*

1.4.1 Le caractère déraisonnable de la fouille, saisie ou perquisition

Au début de l'utilisation de la *Charte*, certains tribunaux ont opiné qu'une fouille illégale ne serait pas nécessairement déraisonnable en vertu de la *Charte*. Selon ces tribunaux, une violation mineure de la loi ne devrait pas justifier l'application de l'article 8 de la *Charte* et l'exclusion de la preuve recueillie[239]. Toutefois,

> « [s]ince the decision of the Supreme Court of Canada in *Collins* and *Kokesh*, it now seems clear that a search that is not legal either under stature of at common law is necessarily unreasonable under s. 8 The question of whether the legal violation is trivial or serious is only relevant to the s. 24(2) inquiry. »[240]

Ainsi, dès qu'il y a violation de la *Charte*, que celle-ci soit mineure ou majeure, la Cour devra procéder à l'analyse requise en vertu du paragraphe 24(2) de la *Charte*.

---

[237] *R.* c. *Fearon*, préc., note 133.
[238] Pierre-Luc DÉZIEL et Alexandre STYLIOS, « La problématique des messages textes historiques : attente raisonnable de vie privée et interception de communications privées », dans *Réformer le droit criminel au Canada: défis et possibilités - Criminal law reform in Canada : challenges and possibilities*, Montréal, Éditions Yvon Blais, 2017, p. 536.
[239] *R.* v. *Heisler*, 1984 ABCA 30, par. 6.
[240] Don STUART et Tom QUIGLEY, *Learning Canadian criminal procedure*, 12e éd., Toronto, Thomson Reuters, 2016, p. 143.

1.4.2 L'exclusion des éléments de preuve obtenus en violation de l'article 8 de la **Charte**

Une revue exhaustive de l'exclusion des éléments de preuve obtenus en violation de l'article 8 de la *Charte* pourrait faire l'objet d'un mémoire entier. Malgré ce constat, il nous semblait impératif de survoler, à tout le moins, les principes applicables, afin de brosser un portrait exact de l'état actuel du droit au sujet des fouilles, saisies et perquisitions.

Bien que le paragraphe 24(1) de la *Charte* puisse également être utilisé afin d'exclure des éléments de preuve, c'est plutôt le paragraphe 24(2) qui s'appliquera lorsque les éléments de preuve ont été obtenus en violation de la *Charte*[241]. Selon cette disposition, les éléments de preuve ainsi obtenus devront être déclarés inadmissibles si leur utilisation est susceptible de déconsidérer l'administration de la justice. Il reviendra à la personne demandant l'exclusion de preuve obtenue en violation de l'article 8 de la *Charte*, donc l'accusé, de démontrer que tel est le cas, selon le fardeau de la prépondérance des probabilités[242].

La Cour suprême a examiné la notion de déconsidération de l'administration de la justice pour la première fois dans l'arrêt *Collins*. En effectuant une compilation des critères les plus souvent utilisés par les tribunaux, l'honorable juge Lamer a regroupé ceux-ci sous trois grandes catégories : les facteurs ayant trait à l'équité du procès, ceux en lien avec la gravité de la violation et ceux se rapportant à l'effet de l'exclusion de la preuve[243]. Par la suite, dix ans plus tard, la Cour est venue préciser l'approche à suivre avec l'arrêt *Stillman*. Dans cette décision, la Cour est simplement venue préciser les critères développés dans *Collins*, en prêtant une attention particulière aux différents types de preuve, incluant la preuve obtenue en mobilisant l'accusé contre lui-même ou encore la preuve qui aurait pu être découverte d'une autre manière[244].

---

[241] *R.* c. *White*, [1999] 2 R.C.S. 417.
[242] *R.* c. *Collins*, préc., note 45, 280.
[243] *Id.*, 284-286.
[244] *R.* c. *Stillman*, préc., note 49.

En 2009, les critères établis dans l'arrêt *Collins* ont été modifiés par les décisions *Grant*[245], *Suberu*[246] et *Harrison*[247] (souvent désignés collectivement sous le vocable de *Trilogie Grant*). La Cour a alors critiqué l'approche préconisée dans *Stillman*, soulignant que la création de catégories de preuve qui sont généralement inadmissibles allait à l'encontre du paragraphe 24(2) de la *Charte*, qui exige que l'analyse se fasse selon l'ensemble des circonstances[248].

Insistant sur l'objectif sociétal et prospectif du paragraphe 24(2) de la *Charte*, la Cour a résumé ainsi la procédure à suivre :

> « Ainsi, le tribunal saisi d'une demande d'exclusion fondée sur le par. 24(2) doit évaluer et mettre en balance l'effet que l'utilisation des éléments de preuve aurait sur la confiance de la société envers le système de justice en tenant compte de : (1) la gravité de la conduite attentatoire de l'État (l'utilisation peut donner à penser que le système de justice tolère l'inconduite grave de la part de l'État), (2) l'incidence de la violation sur les droits de l'accusé garantis par la *Charte* (l'utilisation peut donner à penser que les droits individuels ont peu de poids) et (3) l'intérêt de la société à ce que l'affaire soit jugée au fond. Le rôle du tribunal appelé à trancher une demande fondée sur le par. 24(2) consiste à procéder à une mise en balance de chacune de ces questions pour déterminer si, eu égard aux circonstances, l'utilisation d'éléments de preuve serait susceptible de déconsidérer l'administration de la justice. »[249]

L'application de ces trois critères doit être effectuée au cas par cas, selon la totalité des circonstances[250]. Ainsi, il est possible qu'un critère milite pour l'exclusion de la preuve, tandis qu'un autre soit plus favorable à son admission. Il s'agit d'une analyse contextuelle, où la création de catégories de preuves qui seront automatiquement exclues est à proscrire[251]. *A contrario*, il ne faut pas présumer non plus qu'une preuve qui est pertinente ou essentielle à la preuve de la poursuite sera nécessairement déclarée admissible[252].

---

[245] *R.* c. *Grant*, [2009] 2 R.C.S. 353.
[246] *R.* c. *Suberu*, [2009] 2 R.C.S. 460.
[247] *R.* c. *Harrison*, [2009] 2 R.C.S. 494.
[248] *R.* c. *Grant*, préc., note 246, par. 65.
[249] *Id.*, par. 71.
[250] J. A. FONTANA et D. KEESHAN, préc., note 74, p. 1135.
[251] *Id.*, p. 1173 et suivantes; *R.* c. *Strachan*, [1988] 2 R.C.S. 980, par. 52.
[252] *R.* c. *Buhay*, préc., note 50, par. 71.

Ces critères ont depuis été repris par tous les tribunaux se penchant sur l'exclusion de la preuve obtenue en violation de la *Charte*, y compris dans des dossiers portant sur de la preuve électronique ou numérique. Par exemple, dans la décision *Vu*, la Cour a conclu que la preuve provenant de l'ordinateur de l'accusé, bien que saisi illégalement en contravention de l'article 8 de la *Charte*, devait être admise, notamment puisque les policiers pensaient que le mandat autorisait la fouille et la saisie de l'ordinateur[253]. Au contraire, dans la décision *Boudreau-Fontaine*, la Cour d'appel du Québec a déclaré l'ordinateur de l'accusé – et les données qu'il contenait – inadmissible en preuve[254]. Comme nous verrons en détail à la section 2.3.1 du présent mémoire, l'accusé avait été forcé de révéler son mot de passe aux policiers, par l'entremise d'un mandat de perquisition. La Cour a considéré que les nombreuses violations des droits de l'accusé, la gravité de celles-ci, le fait que la preuve aurait pu être obtenue autrement, ainsi que le « niveau élevé d'attente en matière de vie privée [accordé] aux données informatiques »[255] militaient pour l'exclusion de la preuve.

[253] *R.* c. *Vu*, préc., note 142.
[254] *R.* c. *Boudreau-Fontaine*, préc., note 186.
[255] *Id.*, par. 71.

Chapitre 2 – La saisie de données informatiques

Dans la décision *Wong*[256], la Cour suprême devait se pencher sur la question de la surveillance magnétoscopique effectuée de manière subreptice par les agents de l'État. La Cour a mentionné d'entrée de jeu que

> « les principes énoncés dans l'arrêt *Duarte* embrassent tous les moyens actuels permettant à des agents de l'État de s'introduire électroniquement dans la vie privée des personnes, et tous les moyens que la technologie pourra à l'avenir mettre à la disposition des autorités chargées de l'application de la loi ».[257]

Ainsi, nous pouvons remarquer que dès le début de l'application de l'article 8 de la *Charte* aux nouvelles technologies, un certain principe de neutralité technologique semble émerger des enseignements de la Cour suprême. Cette neutralité a été réitérée récemment dans la décision *Vu* où la Cour suprême a considéré, tel que précédemment mentionné, que les téléphones cellulaires intelligents constituent, tout compte fait, des ordinateurs[258]. La Cour suprême considère donc que les principes généraux applicables aux fouilles, saisies et perquisitions abusives peuvent évoluer et être adaptés aux progrès de la science et des technologies[259].

En effet, les tribunaux ont toujours été en mesure de répondre adéquatement aux problèmes soulevés par les nouvelles technologies, comme le recours à l'imagerie infrarouge[260] ou le fait de mesurer la consommation d'électricité d'un suspect[261], sans avoir à faire table rase sur l'état du droit à propos de l'article 8 de la *Charte*. Nous sommes donc en accord avec les propos de l'auteur Steven Penney lorsqu'il affirme:

> « There is little reason to think that digitization requires a radical reinterpretation of section 8. Technological change inevitably influences constitutional interpretation and application. But for the most part, the foundation set out by the Supreme Court of Canada in digital (and other) section 8 cases over the past two decades provides the conceptual

---

[256] *R.* c. *Wong*, préc., note 1.
[257] *Id.*, 43-44.
[258] *R.* c. *Vu*, préc., note 142, par. 38; *R.* c. *Fearon*, préc., note 133, par. 54.
[259] *R.* c. *Vu*, préc., note 142, par. 1-2; Pour une opinion contraire, voir L. JORGENSEN, préc., note 177.
[260] *R.* c. *Tessling*, préc., note 2.
[261] *R.* c. *Gomboc*, préc., note 24.

> and doctrinal tools needed to achieve reasonable accommodations between competing privacy and law enforcement interests in the digital era. »[262]

Dans ce chapitre, nous examinerons l'application spécifique de l'article 8 de la *Charte* à la saisie de données situées dans un ordinateur ou tout autre appareil électronique. Nous débuterons par l'analyse de l'attente de vie privée envers le contenu des ordinateurs, avant de nous pencher sur les autorisations judiciaires susceptibles de s'appliquer. Nous survolerons ensuite certains cas problématiques qui sont relevés dans la jurisprudence et la doctrine, plus précisément le cas des données protégées par mot de passe, le cas des données cryptées et les difficultés provenant de l'application de la théorie des « objets bien en vue » (*plain view*) aux perquisitions informatiques.

Section 2.1 L'existence d'une attente de vie privée envers le contenu d'un ordinateur

Les ordinateurs font partie intégrante de nos vies. Nous les utilisons pour travailler, nous amuser, communiquer, apprendre et nous construire une identité[263]. C'est pourquoi les ordinateurs occupent maintenant une place importante dans une majorité d'enquêtes criminelles.

Dans la décision *Morelli*, une affaire de possession de pornographie juvénile, le juge Fish souligne qu'« [i]l est difficile d'imaginer une perquisition, une fouille et une saisie plus envahissantes, d'une plus grande ampleur ou plus attentatoires à la vie privée que celles d'un ordinateur personnel. »[264]. Toutefois, dans la décision, la Cour suprême n'analyse pas spécifiquement la question de l'existence d'une attente raisonnable de vie privée envers le contenu d'un ordinateur personnel. On semble plutôt présumer qu'une telle attente existe, sans plus. Cette décision n'applique donc pas l'analyse contextuelle développée par la Cour suprême, mais plutôt une approche qu'on pourrait qualifier de fondée sur des principes[265], ou encore de

---

[262] Steven PENNEY, « The Digitization of Section 8 of the Charter: Reform or Revolution? », (2014) 67-2 *S.C.L.R.* 505, par. 4.
[263] En ce sens, les ordinateurs constituent des « multi-faceted instrumentality without precedent in our society ». Alan D. GOLD, « Applying Section 8 in the Digital World: Seizures and Searches – Prepared for the 7th Annual Six-Minute Criminal Defence Lawyer, Law Society of Upper Canada », (2007) ADGN/RP-211 *Alan Gold Collect. Crim. Law Artic.*, par. 3.
[264] *R.* c. *Morelli*, préc., note 11, par. 2.
[265] F. BLANCHETTE, préc., note 79.

fondée sur la morale[266]. Il n'en demeure pas moins que cette décision est l'arrêt phare lorsqu'il s'agit d'établir qu'un individu possède une attente raisonnable de vie privée envers le contenu de son ordinateur personnel.

Deux ans après la décision *Morelli*, la Cour suprême s'est à nouveau penchée sur la saisie de données contenues dans un ordinateur, cette fois-ci un ordinateur de travail. Dans la décision *Cole*, la Cour a conclu qu'un individu pouvait posséder une attente raisonnable de vie privée envers le contenu d'un ordinateur de travail, bien que celui-ci ne lui appartienne pas, à partir du moment où l'utilisation de l'ordinateur à des fins personnelles était permise ou raisonnablement prévue[267]. Ceci s'explique par le fait que les ordinateurs, qu'ils soient situés au travail ou à la maison, « contiennent des renseignements qui sont significatifs, intimes et qui ont trait à l'ensemble des renseignements biographiques de l'utilisateur »[268]. Bien que l'attente soit moindre dans le cas d'un ordinateur de travail qu'un ordinateur personnel, il demeure que l'attente est raisonnable et rend donc applicable l'article 8 de la *Charte*[269]. Dans ce cas, la reconnaissance de l'attente raisonnable de vie privée était également due au fait que « Cole was granted exclusive possession of the laptop, was permitted to use the laptop for personnal use, and access to its content was restricted by a password. Furthermore, there was no clear privacy policy relating to [employees'] laptops or searches of them »[270].

Dans la décision *Cole*, l'accusé travaillait comme enseignant dans une école secondaire. Alors qu'un technicien effectuait une opération de maintenance sur l'ordinateur utilisé par Cole, il a découvert des images constituant de la pornographie juvénile. Après avoir informé le directeur de l'école, une copie des images a été prise et sauvegardée sur des CDs. L'ordinateur et les CDs

---

[266] Steven PENNEY, « Reasonable Expectations of Privacy and Novel Search Technologies: An Economic Approach », (2007) 97-2 *J. Crim. Law Criminol.* 477, 479. L'auteur critique le test utilisé par les tribunaux américains et canadiens afin de déterminer si une attente raisonnable de vie privée existe. Il soutient que cette approche est fondée sur la morale, ce qui serait questionnable selon lui. Il propose plutôt une analyse économique, analysant le coût-bénéfice des politiques gouvernementales, afin de déterminer si une attente de vie privée devrait être retenue dans certains cas, ou non.
[267] *R.* c. *Cole*, préc., note 94, par. 1.
[268] *Id.*, par. 2.
[269] *Id.*, par. 8-9.
[270] Brock JONES, « Reconciling Reasonable Expectations of Privacy and Modern Technologies: U.S. v. Canadian Approaches », (2011) 83 *Crim. Rep.* 28, 3.

ont ensuite été transmis aux policiers, qui ont procédé à l'analyse des données, sans qu'un mandat n'ait été obtenu[271]. La majorité de la Cour suprême a conclu que la découverte initiale des images par le technicien, ainsi que leur copie sur CD, était légale. En effet, en raison des obligations du directeur de l'école de fournir un milieu d'apprentissage sécuritaire, il pouvait effectuer une vérification de l'ordinateur de l'accusé et transmettre le résultat de leurs recherches à la police[272]. Toutefois, avant d'accéder au contenu de l'ordinateur et des CDs, la police aurait dû obtenir un mandat[273]. Le fait que l'employeur ait autorisé la saisie de l'ordinateur ne peut justifier la violation des droits de l'accusé, puisque la notion de consentement d'un tiers ne peut permettre de passer outre les droits du premier intéressé, en l'occurrence, l'accusé[274].

Quelques années avant la décision *Cole*, la Cour d'appel du Québec avait décidé qu'on ne pouvait reconnaître l'existence d'une attente raisonnable de vie privée envers le contenu d'un ordinateur de travail lorsque d'autres personnes avaient accès à l'ordinateur, de manière non supervisée[275]. Dans la décision *Tremblay*, l'accusé, qui était employé d'un service de police, avait accédé à de la pornographie juvénile à partir de son ordinateur de travail, prétextant enquêter sur ce type de crimes. En l'espèce, la Cour a conclu qu'on ne pouvait reconnaître une attente raisonnable de vie privée envers le contenu de l'ordinateur utilisé par l'accusé, notamment puisque son adjointe pouvait utiliser l'ordinateur à sa guise et que le technicien à l'emploi du poste de police pouvait accéder à l'ordinateur à distance[276]. Bien que rendus avant la décision *Cole*, nous pensons que les enseignements de la Cour d'appel dans cette décision peuvent toujours s'appliquer, principalement puisque ces différents résultats ne font que réitérer que l'existence d'une attente raisonnable de vie privée doit toujours être évaluée au cas par cas. Donc, dans le cas d'un ordinateur de travail, le contexte sera important afin de déterminer si l'article 8 de la *Charte* peut trouver application.

---

[271] *R.* c. *Cole*, préc., note 94, par. 5.
[272] *Id.*, par. 62 et 73.
[273] *Id.*, par. 73.
[274] *Id.*, par. 77.
[275] *Tremblay* c. *R.*, 2003 QCCA 72060.
[276] *R.* c. *Tremblay*, 2001 QCCQ 24412, par. 22.

Toutefois, lorsque l'ordinateur n'appartient pas à l'individu, mais plutôt à une entreprise avec qui ce dernier fait affaire, l'existence d'une attente raisonnable de vie privée est moins certaine. En effet, dans la décision *Plant*, la Cour suprême avait à déterminer si l'accusé pouvait prétendre avoir une attente raisonnable de vie privée envers les données situées dans l'ordinateur de la compagnie d'électricité avec qui il faisait affaire. Dans ce cas précis, la Cour a conclu qu'une telle attente n'existait pas puisque les données ne révélaient pas de détails sur le mode de vie de l'accusé[277]. *A contrario*, si de telles données situées dans l'ordinateur d'un tiers révélaient des « détails intimes sur le mode de vie et les choix personnels de l'individu »[278], une attente raisonnable de vie privée existerait, bien que les données ne soient pas sous le contrôle de l'individu sous enquête[279].

Le nœud du problème sera donc de déterminer si les données détenues par la tierce partie sont « biographiques d'ordre personnel »[280]. Tel que mentionné précédemment, on devra alors s'attarder à l'objet véritable de la fouille, c'est-à-dire non seulement à ce qui semble être, de prime abord, recherché par les forces de l'ordre, mais bien à ce qui est susceptible d'être découvert sur l'individu par cette technique d'enquête[281]. Certains auteurs commencent même à se questionner sur l'impact que peut avoir la *Charte* sur l'information pouvant être recueillie, puis amalgamée, sur un individu, permettant aux forces de l'ordre d'en apprendre beaucoup sur une personne, à partir d'information à première vue banale, qu'elle a volontairement divulguée en ligne, à des entreprises généralement[282].

Le fait que l'appareil électronique soit protégé ou non par un mot de passe n'est pas un facteur ayant une grande influence sur l'attente raisonnable de vie privée. En effet, selon la Cour suprême :

---

[277] *R.* c. *Plant*, préc., note 99, 293.
[278] *Id.*
[279] Comme il a été le cas dans *R.* c. *Spencer*, préc., note 94.
[280] *R.* c. *Plant*, préc., note 99, 293 en anglais, les termes « *biographical core* » sont utilisés.
[281] *R.* c. *Marakah*, préc., note 81, par. 15; S. PENNEY, préc., note 263, par. 39.
[282] Mathew JOHNSON, « Privacy in the Balance - Novel Search Technologies, Reasonable Expectations, and Recalibrating Section 8 », (2012) 58 *Crim. Law Q.* 442; Lon A. BERK, « After Jones, the Deluge: The Fourth Amendment Treatment of Information, Big Data and the Cloud », (2014) 14 *J. High Technol. Law* 1.

> « Je n'accorderai pas beaucoup de poids à ce facteur dans l'évaluation de l'attente subjective d'une personne en matière de vie privée ou pour déterminer si cette attente est raisonnable. La décision d'une personne de ne pas protéger son téléphone cellulaire par un mot de passe n'indique pas qu'elle renonce en quelque sorte aux intérêts importants en matière de respect de sa vie privée qu'elle a généralement sur le contenu de son téléphone : voir, p. ex., *R. c. Rochwell*, 2012 ONSC 5594, 268 C.R.R. (2d) 283, par. 54. Les téléphones cellulaires — verrouillés ou non — mettent en cause des intérêts importants en matière de respect de la vie privée. Mais nous devons aussi garder ce point en perspective. »[283]

Cette conclusion semble fondée en partie sur le rejet de l'analyse fondée sur le risque dans l'arrêt *Duarte*. En ce sens, le risque que quelqu'un accède aux données de manière non autorisée en raison de l'absence de mot de passe n'est pas un facteur à considérer afin de nier la protection offerte par l'article 8 de la *Charte*. De la même manière, le fait qu'une connexion Internet ne soit pas 100% sécurisée, mettant l'accusé à risque de se faire subtiliser ses données par un pirate informatique, ne nous apparaît pas comme un critère pertinent afin de déterminer si une attente raisonnable de vie privée existe.

Toutefois, pouvons-nous présumer qu'un appareil protégé par un mot de passe, ou des données protégées de la même manière, sera nécessairement et absolument l'objet d'une attente raisonnable de vie privée, sans qu'il ne soit nécessaire de se poser davantage de questions? Certains auteurs semblent le penser[284]. À tout le moins, il est évident que cela dénote l'existence d'une attente *subjective* de vie privée que peut prétendre avoir un individu sur le contenu de ses appareils électroniques et sur ses données. Cela influera également, comme nous le verrons, la possibilité et la manière d'obtenir lesdites données[285].

Tel que mentionné à plusieurs reprises, il est clair que ces principes s'appliquent à plusieurs types d'appareils électroniques, comme les ordinateurs et les cellulaires. Bien que la Cour suprême ne l'ait pas précisé de manière explicite, nous pensons que ces principes s'appliquent également aux tablettes et aux montres intelligentes, qui sont également susceptibles de contenir

---

[283] *R.* c. *Fearon*, préc., note 133, par. 53.
[284] Orin S. KERR, « Applying the Fourth Amendment to the Internet: A General Approach », (2009) 62 *Stanford Law Rev.* 1005, 1021.
[285] Voir la section 2.3.1 du présent mémoire.

des données portant sur le mode de vie de l'accusé. De plus, selon la Cour d'appel de la Colombie-Britannique, les données contenues dans les appareils photo numériques sont protégées par l'article 8 de la *Charte*[286].

Section 2.2 La saisie de données contenues dans un ordinateur

À la lumière de ce que nous venons de voir, il apparaît clair que les citoyens canadiens possèdent généralement une attente raisonnable de vie privée à l'égard du contenu de leurs appareils électroniques[287] et, dans certaines situations, une attente de vie privée envers des données situées dans les appareils de tierces parties. Par ailleurs, il est également indéniable que les forces de l'ordre ont un intérêt important à accéder aux données contenues dans des appareils électroniques. En plus des photos et documents que peuvent contenir ces appareils, il est clair que la majorité des communications s'effectuent maintenant en ligne, plutôt que verbalement[288]. La question qui se pose dès lors est de savoir quelle autorisation judiciaire sera susceptible d'autoriser la saisie de ces données.

2.2.1 Les ordonnances judiciaires applicables

Selon la localisation physique des données que les policiers souhaitent obtenir, il sera possible de recourir au mandat de perquisition ou à une des diverses ordonnances de communication prévues au *Code criminel*. Nous allons donc voir les particularités de ces autorisations judiciaires, spécifiquement dans le cas de la saisie de données.

Par ailleurs, il importe de souligner que les agents des douanes canadiennes peuvent fouiller un ordinateur sans obtenir d'autorisation judiciaire préalable, et ce, en vertu des pouvoirs leur étant conférés par la *Loi sur les douanes*[289]. En effet, selon l'alinéa 99(1)a), l'agent de douanes peut

---

[286] *R.* v. *Caron*, 2011 BCCA 56, par. 61.
[287] A. FRIC, préc., note 151.
[288] *R.* v. *Giles*, 2007 BCSC 1147, par. 43.
[289] *Loi sur les douanes*, L.R.C. 1985, c. 1 (2e suppl.).

examiner toute marchandise importée, sans motifs raisonnables de croire à la commission d'une infraction, ce qui inclut les ordinateurs et autres appareils électroniques[290].

2.2.1.1 Le mandat de perquisition

Tel que nous l'avons vu, le mandat de perquisition prévu à l'article 487 C.cr. doit être utilisé lorsque les policiers désirent saisir des biens se trouvant dans un lieu précis. Cette constatation demeure valide lorsque les biens en question sont des appareils électroniques. Toutefois, certaines distinctions s'imposent.

Lors des perquisitions traditionnelles, c'est-à-dire des perquisitions qui ne visent pas de la preuve électronique, les policiers peuvent fouiller tous les contenants se trouvant dans le lieu, tels que classeurs et armoires, et ce, sans que le mandat de perquisition n'ait à spécifier que tel est le cas[291]. Dans la décision *Vu*[292], la Cour suprême a dû se prononcer sur l'application de ce principe à la saisie d'ordinateurs[293]. Selon la Cour, sous la plume de l'honorable juge Cromwell, les particularités liées aux ordinateurs commandent que cette règle générale soit écartée lors de la fouille d'ordinateurs. Quatre distinctions fondamentales entre les ordinateurs et les autres contenants susceptibles d'être fouillés lors de l'exécution d'un mandat de perquisition existent et motivent cette exception :

> « Premièrement, les ordinateurs stockent d'immenses quantités de données, dont certaines, dans le cas des ordinateurs personnels, touchent à l'"ensemble de renseignements biographiques d'ordre personnel" qu'a mentionné notre Cour dans *R.* c. *Plant*, […].
>
> Deuxièmement, comme le soulignent l'appelant et l'intervenante la Criminal Lawyers' Association (Ontario), les ordinateurs renferment des données qui sont générées automatiquement, souvent à l'insu de l'utilisateur. […]
>
> Troisièmement – et ce point est d'ailleurs lié au second –, l'ordinateur conserve des fichiers et des données même après que les utilisateurs croient les avoir détruits. […]

---

[290] A. FRIC, préc., note 151.
[291] J. A. FONTANA et D. KEESHAN, préc., note 74, p. 219.
[292] *R.* c. *Vu*, préc., note 142.
[293] La Cour spécifie que ses conclusions s'appliquent également à la saisie de téléphones cellulaires *Id.*, par. 38.

> Quatrièmement, limiter l'endroit où la fouille se déroule à "un bâtiment, contenant ou lieu" (par. 487(1) du *Code*) ne constitue pas une restriction utile en ce qui concerne la fouille des ordinateurs. […] la fouille d'un ordinateur connecté à Internet ou à un réseau permet d'avoir accès à des données et à des documents qui ne se trouvent pas concrètement dans le lieu où la fouille est autorisée. »[294]

Ainsi, on peut conclure que « the old rules that protected privacy in an Analog World are insufficient in the Digital Age »[295]. Un policier ne peut donc fouiller le contenu d'un ordinateur si le mandat ne spécifie pas que cela est permis. À défaut d'une telle autorisation expresse préalable, les policiers ne pourront que saisir l'ordinateur, sans en examiner le contenu, jusqu'à ce qu'ils obtiennent une nouvelle autorisation judiciaire. Ils pourront toutefois effectuer certaines opérations afin de s'assurer de préserver l'intégrité des données[296]. Par ailleurs, selon la Cour d'appel de l'Ontario, les enseignements de la Cour suprême dans l'arrêt *Vu* s'appliquent également à la saisie de clés USB[297].

Les policiers devront donc obtenir un mandat de perquisition en vertu de l'article 487 C.cr. lorsqu'ils veulent saisir des appareils électroniques se trouvant à l'intérieur d'un lieu spécifique, comme une maison d'habitation ou un établissement commercial. Toutefois, qu'en est-il lorsque l'appareil en question ne se trouve pas dans une résidence ou un autre lieu spécifique ? Les policiers pourront alors vraisemblablement utiliser leurs autres pouvoirs de saisie, tel que la fouille incidente à une arrestation le cas échéant, afin de saisir les appareils électroniques. Appliquant les enseignements de la Cour dans l'arrêt *Vu*, les policiers devront alors obtenir un mandat autorisant la saisie des données avant de pouvoir y accéder, sous réserve des particularités déjà étudiées par rapport à la saisie de téléphones cellulaires lors de fouilles incidentes à une arrestation.

Par ailleurs, selon le paragraphe 487(2.1), toute personne qui exécute un mandat de perquisition visant un ordinateur peut :

---

[294] *Id.*, par. 41-44.
[295] N. R. HASAN, préc., note 152, par. 20.
[296] *R.* c. *Vu*, préc., note 142, par. 49.
[297] *R.* v. *Tuduce*, 2014 ONCA 547, par. 70.

« **a)** utiliser ou faire utiliser tout ordinateur s'y trouvant pour vérifier les données que celui-ci contient ou auxquelles il donne accès;

b) reproduire ou faire reproduire des données sous forme d'imprimé ou toute autre forme intelligible;

c) saisir tout imprimé ou sortie de données pour examen ou reproduction;

d) utiliser ou faire utiliser le matériel s'y trouvant pour reproduire des données. » [298]

De plus, le responsable du lieu de la perquisition doit permettre à l'individu exécutant la perquisition d'effectuer ces opérations[299]. Le sens exact de l'expression « données […] auxquelles [l'ordinateur] donne accès » sera étudié plus amplement dans la section 3.3.1 du présent mémoire, en raison de la possibilité que cette disposition permette d'accéder à des données sauvegardées sur un serveur appartenant à un tiers (infonuagique).

2.2.1.2 Le mandat général

Tel que mentionné, le mandat général de l'article 487.01 C.cr. peut être utilisé afin de pénétrer de manière subreptice dans une résidence[300]. Il semblerait maintenant que cette disposition, ou son équivalent américain du moins, puisse être utilisée afin d'entrer de manière subreptice dans une résidence afin de copier et ensuite analyser des données informatiques[301]. Il serait également possible que cette autorisation judiciaire soit utilisée afin d'activer à distance une caméra sur un ordinateur afin d'identifier l'individu utilisant l'appareil[302]. Il s'agirait alors de l'équivalent virtuel d'installer des caméras cachées dans un endroit avec un mandat général.

2.2.1.3 Les ordonnances de communication

Si les données se trouvent dans l'ordinateur d'un tiers qui n'est pas visé par l'enquête, les policiers pourront alors utiliser les diverses ordonnances de communication prévues au *Code*

---

[298] *Code criminel*, préc., note 17, art. 487(2.1).
[299] *Id.*, art. 487(2.2).
[300] *Shooner* c. *R.*, préc., note 201.
[301] Joel ROTHMAN, « Sneak and Peek Warrants », (2001) *Alan Gold Collect. Crim. Law Artic.* 356.
[302] Il serait en effet très facile d'activer à distance une caméra, que ce soit par les policiers ou par des pirates informatiques. Voir Mohit KUMAR, « FBI Director — You Should Cover Your Webcam With Tape », *The Hacker News*, en ligne : <https://thehackernews.com/2016/09/hacking-webcam-cover.html> (consulté le 9 avril 2018).

criminel afin d'accéder aux données. Selon le type de données recherchées, les policiers devront utiliser l'ordonnance spécifique s'appliquant, ou encore l'ordonnance générale de communication.

A) L'ordonnance de communication en vue de retracer une communication spécifique

Cette ordonnance de communication, prévue à l'article 487.015 C.cr., permet aux policiers d'obtenir des adresses courriel, des adresses de protocole Internet (IP)[303] ou des adresses MAC[304]. Le but de cette disposition est de « déterminer l'origine d'une télécommunication »[305], en identifiant « tout dispositif ayant servi à la transmission de la communication ou toute personne y ayant participé »[306]. En obtenant une telle autorisation judiciaire, les policiers ne pourront toutefois obtenir le contenu des communications[307]. Cette disposition existait avant l'adoption du projet de loi C-13[308], mais a été modifiée à ce moment.

B) L'ordonnance de communication pour des données de transmission

L'ordonnance de communication pour données de transmission, prévue à l'article 487.016 C.cr. permet d'obtenir, comme son nom l'indique, des données de transmission. Cette expression est définie comme étant :

> « Données qui, à la fois :

---

[303] L'adresse IP est une adresse unique qui identifie un appareil électronique et qui est utilisé pour communiqué dans un réseau. On peut comparer celle-ci à une adresse résidentielle. Voir IP LOCATION, « What is my IP address? », en ligne : <https://www.iplocation.net/find-ip-address> (consulté le 31 mars 2018).
[304] L'adresse MAC étant « l'adresse physique de la carte réseau », qui est normalement unique. Voir CCM, « Trouver son adresse MAC » (mars 2018), en ligne : <http://www.commentcamarche.com/faq/10935-trouver-son-adresse-mac> (consulté le 31 mars 2018); COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, préc., note 222.
[305] Julia NICOL et Dominique VALIQUET, « Résumé législatif du projet de loi C-13 : Loi modifiant le Code criminel, la Loi sur la preuve au Canada, la Loi sur la concurrence et la Loi sur l'entraide juridique en matière criminelle », p. 14, en ligne : Bibliothèque du Parlement <http://www.bdp.parl.gc.ca/content/lop/LegislativeSummaries/41/2/c13-f.pdf> (consulté le 8 novembre 2016).
[306] *Code criminel*, préc., note 17, art. 487.015.
[307] J. NICOL et D. VALIQUET, préc., note 306, p. 14.
[308] *Loi modifiant le Code criminel, la Loi sur la preuve au Canada, la Loi sur la concurrence et la Loi sur l'entraide juridique en matière criminelle*, préc., note 205.

> **a)** concernent les fonctions de composition, de routage, d'adressage ou de signalisation en matière de télécommunication;
>
> **b)** soit sont transmises pour identifier, activer ou configurer un dispositif, notamment un programme d'ordinateur au sens du paragraphe 342.1(2), en vue d'établir ou de maintenir l'accès à un service de télécommunication afin de rendre possible une communication, soit sont produites durant la création, la transmission ou la réception d'une communication et indiquent, ou sont censées indiquer, le type, la direction, la date, l'heure, la durée, le volume, le point d'envoi, la destination ou le point d'arrivée de la communication;
>
> **c)** ne révèlent pas la substance, le sens ou l'objet de la communication. »[309]

Il peut donc s'agir d'« adresse d'IP, domaines et pages de sites Web visités, protocoles de partage de fichiers et autres, numéros de paquets, termes de recherche dans les moteurs de recherche et adresse de courriel »[310]. Ces données pourront ensuite être utilisées afin d'obtenir une ordonnance de communication en vue de retracer une communication spécifique[311].

Cette ordonnance, toute comme l'ordonnance de communication pour données de localisation, ne peut être utilisée que pour obtenir des données déjà en possession de l'organisme visé par la demande lorsqu'il reçoit l'ordonnance. Pour obtenir des données futures en temps réel, un mandat devra plutôt être obtenu par les forces de l'ordre[312].

C) L'ordonnance de communication pour des données de localisation

Les données de localisation sont définies comme étant des « [d]onnées qui concernent le lieu d'une opération ou d'une chose ou le lieu où est située une personne physique »[313]. Il va donc souvent s'agir de coordonnées GPS[314], comme dans la décision *R.* v. *Edwards* où cette disposition a été utilisée afin d'obtenir le registre des coordonnées GPS d'une voiture que

---

[309] *Code criminel*, préc., note 17, art. 487.011.
[310] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, préc., note 222.
[311] J. NICOL et D. VALIQUET, préc., note 306, p. 14.
[312] *Id.*
[313] *Code criminel*, préc., note 17, art. 487.011.
[314] Le système GPS (pour *Global Positioning System*) permet de connaître l'emplacement géographique de tout appareil muni d'une telle fonction. Il est opéré par le gouvernement américain. Voir « GPS: The Global Positioning System », en ligne : <https://www.gps.gov/> (consulté le 31 mars 2018).

l'accusé avait louée[315]. Il pourrait également s'agir des coordonnées GPS d'un cellulaire, obtenues grâce aux tours cellulaires.

D) L'ordonnance de communication pour des données financières

Cette ordonnance de communication est prévue à l'article 487.018 C.cr. Ce type d'ordonnance de communication n'est pas nouveau et existait avant les modifications apportées par le projet de loi C-13, à l'ancien article 487.013 C.cr.

Cette disposition permet aux policiers d'accéder aux « renseignements sur le titulaire du compte, [aux] types de compte, [à la] date de création du compte et [à l']adresse courante »[316]. L'ordonnance peut être adressée à toute institution financière au sens de l'article 2 de la *Loi sur les banques*[317] ou à toute entité ou personne visée à l'article 5 de la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes*[318].

E) L'ordonnance générale de communication

Tel que mentionné, les ordonnances spécifiques de communication étudiées ci-dessus ne permettent pas aux policiers d'avoir accès au contenu des conversations, mais plutôt aux données entourant celles-ci. Ainsi, si les policiers désirent accéder au contenu de conversations terminées, tel que le texte contenu dans un courriel arrivé à destination, en passant par un FSI, ils devront employer l'ordonnance générale de communication, prévue à l'article 487.014 C.cr., ce qui implique que les policiers devront satisfaire au critère plus exigeant des « motifs raisonnables de *croire* », plutôt que des « motifs raisonnables de *soupçonner* »[319]. Au contraire, si les policiers désirent accéder au contenu de conversations en cours, en temps réel, ils devront

---

[315] *R.* v. *Edwards*, 2015 ONCJ 347.
[316] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, préc., note 222.
[317] *Loi sur les banques*, L.C. 1991, c. 46.
[318] *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes*, L.C. 2000, c. 17.
[319] Par analogie à *R.* c. *Jones*, préc., note 53, il est possible de conclure que les courriels déjà arrivés à destination, comme les messages textes, peuvent être obtenus par une ordonnance générale de communication.

utiliser les dispositions de la partie VI du *Code criminel*, en matière d'interception des communications privées[320].

Par ailleurs, comme cela a été mentionné, les renseignements relatifs à l'abonné, tels que son nom, adresse et numéro de téléphone, doivent également être obtenus par le biais d'une ordonnance générale de communication, non pas une des ordonnances de communication spécifiques[321].

2.2.2 La procédure à suivre lors de la saisie des données

Lorsque les policiers exécutent un mandat de perquisition visant un ordinateur, certaines règles précises dictent la procédure à suivre. Ces règles sont directement liées à la troisième condition posée par l'arrêt *Colins* afin qu'une perquisition respecte l'article 8 de la *Charte*, soit qu'elle ne soit pas effectuée de manière abusive[322].

Tout d'abord, il est utile de préciser que les policiers, lorsqu'ils sont autorisés à fouiller un ordinateur, n'ont pas l'obligation de fouiller le contenu de celui-ci sur les lieux de la perquisition. En effet, selon la décision *Weir*, les données peuvent être extraites de l'appareil électronique à un autre endroit que celui où a eu lieu la perquisition et à une date ultérieure, tant que la saisie a été effectuée de manière adéquate[323].

Après que le mandat de perquisition ait été exécuté et que les appareils électroniques aient été saisis par les policiers, l'enquêteur attitré à la saisie des données[324] devra tout d'abord s'assurer de créer des copies miroirs des données sauvegardées dans l'ordinateur[325]. Cette étape cruciale permettra au ministère public de respecter les exigences en matière de fiabilité et d'authenticité de la preuve, en vertu de la *Loi sur la preuve au Canada*[326]. Ainsi, si elle le désire, la défense

---

[320] *R.* c. *Société TELUS Communications*, préc., note 195, par. 12; *R.* c. *Jones*, préc., note 53, par. 81.
[321] *Re Subscriber Information*, préc., note 217.
[322] *R.* c. *Collins*, préc., note 45, 278.
[323] *R.* v. *Weir*, 2001 ABCA 181, par. 19.
[324] Habituellement, il s'agira d'un enquêteur spécialisé en preuve électronique (*digital forensics investigator*). John J BARBARA, *Handbook of digital and multimedia evidence*, Totowa, Humana, 2007.
[325] Orin S. KERR, « Searches and seizures in a digital world », 119 *Harv. Law Rev.* 531, 540.
[326] *Loi sur la preuve au Canada*, L.R.C. 1985, c. C-5.

pourra consulter sa propre copie des données afin de constater qu'elles n'ont pas été altérées. Par ailleurs, le mode de fonctionnement des ordinateurs peut également modifier la preuve numérique, sans intention de la part de l'usager. En effet, le simple fait d'ouvrir un document va venir modifier certaines métadonnées (*metadata*)[327] qui peuvent être pertinentes pour l'enquête[328]. En créant une copie miroir, les enquêteurs pourront donc s'assurer que les métadonnées, selon l'état où elles se trouvaient lors de la perquisition, peuvent être consultées. De plus, il est possible de venir contre-vérifier la validité de la copie miroir créée par les policiers en utilisant la valeur de hachage (*hash value*)[329] d'un document[330]. Si les valeurs de hachages comparées sont différentes, on peut conclure que les données d'origine ont été modifiées depuis leur saisie, faisant en sorte que l'authenticité de la preuve sera plus difficile à établir ou ne pourra pas l'être[331].

Après que cette phase d'acquisition des données ait été complétée, vient la phase d'examen des données, aussi appelée *data reduction phase* par certains auteurs[332]. C'est à cette étape que les enquêteurs vont fouiller l'ensemble des données copiées[333] et tenter de découvrir la preuve pertinente à leur enquête. De manière générale, il est possible de résumer ainsi les divers gestes posés par l'enquêteur chargé d'examiner des données électroniques :

> « 1. Nonintrusive acquisition of a replicated image of data extracted from the questioned device. This is typically termed the *forensic image*.
>
> 2. Calculation of the authentication hash value necessary to properly authenticate the data stored on both the questioned device and the forensics image.

---

[327] Les métadonnées peuvent être définies comme « des données qui portent sur des données ». Il s'agit par exemple de la date de création d'un fichier ou de son volume. Voir « What is metadata? - Definition from WhatIs.com », *WhatIs.com*, en ligne : <http://whatis.techtarget.com/definition/metadata> (consulté le 31 mars 2018).
[328] N. R. HASAN, préc., note 152, par. 78.
[329] La valeur de hachage est constituée d'une série de chiffres qui identifient de manière unique des données. Voir MICROSOFT, « Ensuring Data Integrity with Hash Codes », en ligne : <https://docs.microsoft.com/en-us/dotnet/standard/security/ensuring-data-integrity-with-hash-codes> (consulté le 31 mars 2018).
[330] O. S. KERR, préc., note 326, 541.
[331] *Loi sur la preuve au Canada*, préc., note 327, art. 31.1.
[332] O. S. KERR, préc., note 326, 547.
[333] L'analyse de la preuve est effectuée à partie des copies seulement, pour éviter de compromettre les données originales. *Id.*, 540.

3. Conducting a file-fragment recovery procedure to “undelete” files, folders, and directory objects.

4. Performing a hash file signature analysis to note file attributes.

5. Recovering temp, swap, file slack, and page objects.

6. Searching for file hash values—known and unknown filters.

7. Searching for key-term strings.

8. Reviewing file notations.

9. Noting applications or indications of file manipulation activity such as file eradicators, encryption, file compressors, or file hiding utilities.

10. Reviewing typical evidentiary objects such as:

A. Application software applications

B. Digital camera, printer, and ancillary storage devices

C. E-mails

D. Games

E. Graphics images

F. Internet chat logs

G. Latent data extraction from slack, page, temp, and registry spaces

H. Network activity logs

I. Recycle folders

J. System and file date/time objects

K. User-created directories, folders, and files

11. Preparing evidence summaries, exhibits, reports, and expert findings based on evidentiary extracts and investigative analysis. »[334]

---

[334] Larry R. LEIBROCK, « Duties, Support Functions, and Competencies: Digital Forensics Investigators », dans *Handbook of Digital and Multimedia Forensic Evidence*, Totowa, Humana Press, 2008, p. 92.

Une fois la preuve recueillie et analysée, elle pourra être utilisée lors du procès de l'accusé. Le policier ayant effectué l'analyse de la preuve devra habituellement venir présenter sa méthode de travail à la Cour, à moins que les parties n'aient consenti à son admission en preuve, d'où l'importance que des notes détaillées soient prises lors de la fouille[335].

Section 2.3 Les cas problématiques

Certaines situations peuvent rendre plus ardue la collecte de données après la saisie des appareils électroniques. Trois éventualités retiennent notre attention, soit le cas des données protégées par un mot de passe, le cas des données cryptées et l'application de la théorie des « objets bien en vue » à la saisie de données informatiques.

2.3.1 Le cas des données protégées par un mot de passe

Bien que la Cour suprême ait décidé que l'existence ou non d'un mot de passe protégeant des appareils électroniques n'ait pas une incidence importante sur l'existence d'une attente raisonnable de vie privée[336], cet élément n'est pas sans incidence pour les forces de l'ordre. En effet, l'existence d'un mot de passe peut compliquer le travail policier, voire même l'empêcher complètement.

Ce scénario ne relève pas seulement de la fiction. Aux États-Unis, les autorités de San Bernardino en Californie ont été confrontées à ce problème après avoir découvert un téléphone *iPhone* protégé par un mot de passe et par cryptage, après un attentat ayant fait plusieurs morts[337]. L'entreprise *Apple*, fabricant du téléphone, a refusé de fournir les mots de passe qui auraient permis aux policiers d'accéder aux données, obligeant le *Federal Bureau of Investigation* (FBI) d'avoir recours aux services chers payés d'un consultant qui serait en fait

---

[335] À ce sujet, la Cour suprême n'a pas conclu que la prise de note était nécessaire au plan constitutionnel, mais qu'elle était néanmoins souhaitable. *R.* c. *Vu*, préc., note 142, par. 70.
[336] *R.* c. *Fearon*, préc., note 133, par. 57.
[337] Arjun KHARPAL, « Apple vs FBI: All you need to know » (29 mars 2016), en ligne : <https://www.cnbc.com/2016/03/29/apple-vs-fbi-all-you-need-to-know.html> (consulté le 14 avril 2018).

un pirate informatique[338]. Bien que le téléphone ait finalement été déverrouillé, cette situation soulève plusieurs interrogations par rapport aux options qui s'offrent aux policiers dans ce genre de dossier.

L'état du droit au Québec semble clair sur la question de savoir si on peut forcer un suspect à fournir son mot de passe de manière verbale ou écrite aux policiers. En effet, la Cour d'appel du Québec, dans la décision *Boudreau-Fontaine*, a clairement refusé qu'un juge force un individu à fournir son mot de passe aux policiers, par l'entremise d'un mandat de perquisition[339]. Selon la Cour, cette condition du mandat de perquisition contrevenait directement au droit au silence et au droit contre l'auto-incrimination dont jouit l'accusé et ne pouvait être justifiée par les paragraphes 487(2.1) et (2.2.) C.cr. [340]. La Cour souligne également que la preuve ne révélait pas si les policiers auraient pu avoir autrement accès à l'ordinateur, sans forcer l'accusé à s'incriminer de la sorte[341]. L'état du droit aux États-Unis semble être le même quant à la possibilité de forcer un individu à fournir son mot de passe verbalement ou par écrit aux autorités[342].

Quelles autres options s'offrent donc aux policiers devant un appareil protégé par un mot de passe? Ils pourront bien évidemment essayer de déverrouiller les appareils saisis autrement, soit en recourant à des logiciels particuliers, à des experts en informatique ou simplement en fonctionnant par essai-erreur. Ils pourront également tenter de saisir d'autres appareils ou des notes manuscrites, sur lesquels les mots de passe pourraient être indiqués[343].

Dans certains cas, il se pourrait qu'une tierce partie soit en mesure d'accéder au mot de passe. Une autorisation judiciaire pourrait-elle alors être utilisée afin d'obtenir celui-ci? Selon l'auteure Sarah Wilson, les mots de passe font définitivement l'objet d'une attente raisonnable de vie

---

[338] Mark HOSENBALL, « FBI paid under $1 million to unlock San Bernardino iPhone: sources », *Reuters* (4 mai 2016), en ligne : <https://www.reuters.com/article/us-apple-encryption/fbi-paid-under-1-million-to-unlock-san-bernardino-iphone-sources-idUSKCN0XQ032> (consulté le 14 avril 2018).
[339] *R.* c. *Boudreau-Fontaine*, préc., note 186, par. 46.
[340] *Id.*, par. 46 et 59.
[341] *Id.*, par. 44.
[342] Dan TERZIAN, « The Micro-Hornbook on the Fifth Amendment and Encryption », 104 *Georgetown Law J.* 168, 170.
[343] *R.* v. *Stemberger*, 2012 ONCJ 31, par. 51.

privée, bien qu'ils aient été partagés avec une tierce partie, en l'occurrence le FSI[344]. Cette constatation est particulièrement pertinente aux États-Unis, où la *third party doctrine* peut nier l'existence même d'une attente raisonnable de vie privée dès que l'information a été révélée à un tiers[345]. Cependant, selon elle, la protection offerte par la Constitution américaine – que ce soit en matière de fouilles, saisies et perquisitions abusives ou en matière de droit contre l'auto-incrimination – n'empêche pas les forces de l'ordre d'obtenir un mot de passe directement d'un FSI[346].

À l'instar de l'auteure, nous pensons que les mots de passe font effectivement l'objet d'une attente raisonnable de vie privée, notamment en raison des informations privées que leur utilisation peut révéler, du fait que les individus ne divulguent habituellement pas leurs mots de passe à n'importe qui et puisqu'on ne pense généralement pas qu'un FSI pourra être contraint de divulguer ceux-ci. À tout le moins, une autorisation judiciaire serait donc nécessaire afin d'obtenir des mots de passe par l'entremise d'un FSI. Dans ce cas, l'ordonnance générale de communication devrait être utilisée, puisqu'aucune autre disposition spécifique ne vise les mots de passe[347]. Malgré cette constatation, il est utile de préciser que la majorité des fabricants d'appareils électroniques ne conservent pas le mot de passe que l'usager utilise afin d'accéder à l'appareil. Ce ne seront donc que les mots de passe de comptes en ligne, tels que les comptes courriel ou des comptes de réseaux sociaux, qui pourront être obtenus par ordonnance de communication.

Certaines questions demeurent en suspens au Canada sur le sujet des mots de passe. En effet, alors qu'aux États-Unis il a été décidé qu'un individu pouvait légalement être contraint à déverrouiller son téléphone à l'aide de son empreinte digitale[348], nous n'avons répertorié aucune

---

[344] Sarah WILSON, « Compelling Passwords from Third Parties: Why the Fourth and Fifth Amendments Do Not Adequately Protect Individuals When Third Parties Are Forced to Hand over Passwords », (2015) 30 *Berkeley Technol. Law J.* 1.
[345] *Id.*, 15.
[346] *Id.*, 33.
[347] Voir annexe I.
[348] S. WILSON, préc., note 344, 28; D. TERZIAN, préc., note 342, 169.

décision canadienne sur le sujet[349] ni à propos d'autres mesures de protection biométriques[350]. L'utilisation de logiciels ou d'appareils enregistreurs de frappe – qui permettent d'obtenir les touches tapées par un individu afin de deviner ses mots de passe[351] – ne semble pas non plus avoir été examinée par un tribunal canadien siégeant en matière criminelle et pénale[352]. Nous pensons toutefois que ces questions se retrouveront inévitablement devant les tribunaux sous peu, en raison des intérêts importants en matière de vie privée qu'elles soulèvent et du recours grandissant à ce type de technologie.

2.3.2 Le cas des données cryptées

Intimement lié à la question des mots de passe, le cryptage de données (ou chiffrement de données) – défini comme une « opération par laquelle est substitué, à un texte clair, un texte inintelligible, inexploitable pour quiconque ne possède pas la clé permettant de le ramener à sa forme initiale »[353] – est également une préoccupation grandissante pour les forces de l'ordre[354]. Un auteur soutient même que le défi auquel fera face le droit criminel canadien dans les prochaines années par rapport aux nouvelles technologies ne sera pas axé sur le droit contre les fouilles, perquisitions et saisies abusives, mais plutôt sur le droit contre l'auto-incrimination,

---

[349] La décision *R.* v. *Smith*, 2017 ONSC 4683 porte vaguement sur ce sujet. Toutefois, la Cour focus son analyse sur le consentement de l'accusé à la fouille de son téléphone, qu'il a déverrouillé avec son empreinte digitale, et non sur la possibilité qu'un accusé soit forcé à ouvrir son téléphone de la sorte.

[350] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, « Des données au bout des doigts : La biométrie et les défis qu'elle pose à la protection de la vie privée » (1 novembre 2011), en ligne : <https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/renseignements-sur-la-sante-renseignements-genetiques-et-autres-renseignements-sur-le-corps/gd_bio_201102/> (consulté le 14 avril 2018).

[351] WIKIPEDIA, « Keystroke logging », dans Wikipedia, en ligne : <https://en.wikipedia.org/w/index.php?title=Keystroke_logging&oldid=831183322> (consulté le 14 avril 2018).

[352] L'équivalent américain du mandat général aurait toutefois été utilisé pour ce faire. Voir J. ROTHMAN, préc., note 302; Timothy A. WISEMAN, « Encryption, Forced Decryption, and the Constitution », (2015) 11 *J. Law Policy Inf. Soc.* 525, 535-536.

[353] OFFICE QUÉBÉBOIS DE LA LANGUE FRANÇAISE, « Chiffrement » (2013), en ligne : <https://www.oqlf.gouv.qc.ca/ressources/bibliotheque/dictionnaires/terminologie_sec_informatique/chiffrement.html> (consulté le 25 septembre 2018).

[354] Susan W. BRENNER, « Encryption, Smart Phones, and the Fifth Amendment », (2012) 33 *Whittier Law Rev.* 525, 533.

qui est protégé notamment par l'article 7 de la *Charte* à titre de principe de justice fondamentale, en raison de l'augmentation importante des technologies de cryptage de données[355].

Le cryptage de données peut prendre plusieurs formes. Il est possible de crypter les données qui se trouvent dans nos appareils personnels, tels que téléphones et ordinateurs, mais également nos activités en ligne, par exemple nos communications[356]. De plus, lorsqu'il est question de cryptage de données, il est possible de crypter un disque dur en entier (*disk-level encryption*), ou encore seulement certains fichiers précis (*file-level encryption*)[357]. Lorsque les données sont cryptées, il arrivera parfois que certaines informations soient tout de même disponibles sur l'appareil électronique, par exemple le nom du fichier[358]. Bien qu'utilisé afin de dissimuler des informations de nature criminelle, le cryptage permet également de poser plusieurs gestes parfaitement légaux, comme d'effectuer des transactions en ligne de manière sécuritaire, que ce soit des achats ou des transactions bancaires[359].

Le programme *Pretty Good Privacy* (PGP) était l'un des logiciels de cryptage les plus répandus et considéré parmi les plus difficiles à contourner[360]. Une fois les données cryptées, en théorie, seuls un mot de passe ou une clé d'accès permettent d'avoir accès aux données dans un format lisible[361]. Toutefois, il a maintenant été révélé que les autorités avaient été capables de contourner les mesures de protection du programme, notamment dans le cadre d'une vaste enquête criminelle portant sur le crime organisé au Canada[362]. Le logiciel *Silent Circle* permet à ses utilisateurs de crypter leurs données directement à partir de leur téléphone, que ce soit leurs

---

[355] Nicola DALLA GUARDA, « Digital Encryption and the Freedom from Self-incrimination: Implications for the Future of Canadian Criminal Investigations and Prosecutions », (2014) 61 *Crim. Law Q.* 119, 120.
[356] *Id.*, 122.
[357] Benjamin Folkinshteyn, « A Witness against Himself: A Case for Stronger Legal Protection of Encryption », (2013) 30 *St. Clara High Technol. Law J.* 414, 379.
[358] *R.* v. *Burke*, 2015 SKPC 173, par. 8.
[359] T. A. WISEMAN, préc., note 353, 525.
[360] J. ROTHMAN, préc., note 302.
[361] *Id.*
[362] Jordan PEARSON et Justin LING, « Exclusive: How Canadian Police Intercept and Read Encrypted BlackBerry Messages », *Motherboard* (14 avril 2016), en ligne: <https://motherboard.vice.com/en_us/article/mg77vv/rcmp-blackberry-project-clemenza-global-encryption-key-canada> (consulté le 25 septembre 2018); John ZORABEDIAN, « Police say they can read Blackberry PGP encrypted email », *Naked Security* (13 janvier 2016), en ligne : <https://nakedsecurity.sophos.com/2016/01/13/police-say-they-can-crack-blackberry-pgp-encrypted-email/> (consulté le 25 septembre 2018).

données sur Internet ou encore leurs communications[363]. Dans la décision *Sonne*, la Cour supérieure de l'Ontario a noté la présence du logiciel *TrueCrypt* dans l'ordinateur de l'accusé, sans pouvoir conclure de manière non équivoque que ce logiciel avait permis le cryptage des données de l'accusé. Malgré des tentatives de la part des policiers, les données n'avaient pu être décryptées[364]. Quant à lui, le logiciel *GNU Privacy Guard* permet de crypter le contenu de courriels, laissant toutefois l'existence même du courriel et les adresses de l'expéditeur et du récipient visibles pour un observateur[365]. D'autres logiciels similaires existent également et plusieurs sont disponibles gratuitement en ligne[366]. Concrètement, l'utilisation de ces technologies pourra parfois empêcher les forces de l'ordre d'avoir accès aux données, puisqu'elles ne seront pas capables de contourner ces mesures de protection.

De façon générale, le problème du cryptage de données est le même que celui des mots de passe. En effet, en utilisant le bon mot de passe ou la bonne clé d'accès, il est possible de décrypter les données pour être capable de les consulter[367]. Dans la décision *Stemberger*, le policier chargé de rédiger la dénonciation au soutien d'un mandat de perquisition a très bien résumé comment les deux concepts se rejoignent :

> « Passwords can be used by computer systems and computer programs to protect data. Several computer manufacturers offer password protection on computer laptop hard disc drives. The user is prompted for a password when the computer is first turned on. If the correct password is not provided, the hard disc drive will not operate and the data is unreadable. Presently, there exists no technique to defeat this "lock-out" feature. In addition, widely available encryption programs (e.g. Truecrypt) are capable, with a sufficiently robust password, of providing near absolute protection of data from viewing by other users. It simply may be impossible to "crack" the password. Without the password, the encrypted file cannot be read. […] »[368]

S'inquiétant de la possibilité que les policiers ne puissent tout simplement pas rivaliser avec les criminels, il a été proposé que le cryptage infaillible, soit celui qui est impossible à contourner

---

[363] N. DALLA GUARDA, préc., note 356, 123.
[364] *R. v. Sonne*, 2012 ONSC 2126.
[365] B. FOLKINSHTEYN, préc., note 357, 379.
[366] *Id.*
[367] N. DALLA GUARDA, préc., note 356, 122.
[368] *R.* v. *Stemberger*, préc., note 344, par. 51. Bien que non mentionné dans la décision *Stemberger*, ce passage semble issu de la décision *R.* v. *Bishop*, 2007 ONCJ 441, par. 49.

même pour l'entreprise l'ayant inventé[369], soit tout simplement banni. Il s'agirait donc d'obliger les entreprises qui créent des logiciels et des appareils électroniques à inclure une porte d'accès dans leurs appareils, qui permettrait aux forces de l'ordre de contourner le cryptage d'un appareil. En 2014, le directeur du FBI a proposé l'adoption de lois qui forcerait les entreprises à inclure une telle porte d'accès dans leurs appareils, sous la forme d'une clé qui serait connue par le gouvernement. Les forces de l'ordre pourraient ensuite utiliser la clé lorsque nécessaire dans le cadre d'une enquête criminelle, après avoir obtenu une autorisation judiciaire[370]. Cette proposition a été vivement critiquée par les dirigeants d'entreprises qui soulignent qu'on ne peut laisser une porte d'accès dans un logiciel qui sera seulement utilisée par le gouvernement, sans aucun risque que les pirates informatiques n'en bénéficient également[371].

La constitutionnalité d'une telle mesure est évidemment difficile à confirmer pour le moment. Il a été suggéré que de restreindre par voie législative les possibilités de cryptage de données serait contraire au Quatrième amendement américain, l'équivalent de l'article 8 de la *Charte*, en raison du texte même de la disposition qui prévoit un droit positif d'être protégé contre les fouilles abusives[372]. Au contraire, certains auteurs pensent que le gouvernement devrait être en mesure d'accéder aux données cryptées, que ce soit en obtenant le mot de passe utilisé ou en obtenant par *subpoena* une copie décryptée des données, afin de rétablir le droit de l'État de faire enquête pour ces crimes qui autrement resteraient impunis[373]. Selon un auteur canadien, un accusé qui ne témoigne pas à son procès ne pourrait être forcé de fournir une copie décryptée de ses données, en raison du paragraphe 11c) et de l'article 7 de la *Charte*[374]. Selon le même auteur, un témoin qui devrait fournir de telles données décryptées serait également protégé par la *Charte*, cette fois-ci en vertu de l'article 13[375].

---

[369] Les méthodes de cryptage utilisées par Apple et Google seraient si fortes que même ces entreprises ne peuvent décrypter l'information. Steven B. TAYLOR, « Can You Keep a Secret: Some Wish to Ban Encryption Technology for Fears of Data Going Dark », (2016) 19 *SMU Sci. Technol. Law Rev.* 215, 218.
[370] *Id.*, 219.
[371] *Id.*, 219-220.
[372] *Id.*, 227.
[373] Dan TERZIAN, « The Fifth Amendment, Encryption, and the Forgotten State Interest », (2013) 61 *UCLA Law Rev. Discourse* 298.
[374] N. DALLA GUARDA, préc., note 356, 137.
[375] *Id.*, 136.

Concernant spécifiquement l'exécution d'un mandat de perquisition visant un ordinateur protégé par un mot de passe ou par cryptage, la Cour du banc de la Reine de l'Alberta a conclu qu'un second mandat n'était pas nécessaire lorsque les méthodes de protection sont découvertes. Ainsi:

> « once the warrant authorized the search, absent some form of limitation in the warrant, the entirety of the computer's contents could be examined. Accordingly, a new warrant was not necessary to overcome levels of security, encryption, fragmentation, password protection or deletion in relation to the information the laptop contained. »[376]

Il est également utile de souligner que la Cour supérieure de l'Ontario et la Cour provinciale de la Saskatchewan ont noté qu'on ne pouvait tirer d'inférences négatives du fait qu'un individu ait crypté ses données[377]. En effet, bien que le cryptage puisse servir à dissimuler des preuves reliées à un acte criminel, il peut également être utile pour empêcher l'accès à des informations personnelles non criminelles, telles que des relevés bancaires. Par ailleurs, il a déjà été imposé à des accusés, dans le cadre d'une probation, de ne pas faire usage de logiciels de cryptage[378] ou encore de fournir les clés de cryptage aux agents de probation[379].

*2.3.3 L'étendue de la fouille et l'application de la théorie des « objets bien en vue » (***plain view***) à la saisie de données informatiques*

Lors de l'audition devant la Cour suprême dans le dossier *Vu*, l'Association des libertés civiles de la Colombie-Britannique a demandé à la Cour que des protocoles de perquisition soient prévus dans les mandats émis à l'égard d'ordinateurs puisque ceux-ci permettraient « d'encadrer la façon dont les policiers effectuent leurs fouilles et de protéger ainsi certaines parties des ordinateurs du regard des enquêteurs »[380]. Les protocoles pourraient ainsi limiter la fouille à

---

[376] *R.* v. *Twitchell*, 2010 ABQB 693, par. 32.
[377] *R.* v. *Sonne*, préc., note 364, par. 19; *R.* v. *Burke*, préc., note 358, par. 17.
[378] *R.* v. *Wilson*, 2014 BCSC 663; *R.* v. *H.T.*, 2010 MBPC 8.
[379] *R.* v. *Duff*, 2010 ONCJ 493.
[380] *R.* c. *Vu*, préc., note 142, par. 53.

l'utilisation de certains mots-clés, à la recherche de certains types de fichiers, aux fichiers contenus dans une échéance précise ou encore à certains logiciels prédéterminés[381].

En dépit de cet argument intéressant, la Cour a conclu que de tels protocoles ne sont généralement pas requis par l'article 8 de la *Charte*, et ce, pour deux raisons. Premièrement, le contrôle *a posteriori* de la manière qu'une fouille a été effectuée serait plus propice, selon la Cour, « à l'élaboration de nouvelles règles sur la façon d'effectuer les fouilles que ne l'est la procédure *ex parte* de délivrance des mandats »[382]. La jurisprudence portant sur cette question peut ensuite être utilisée par le législateur, s'il le souhaite, afin de créer des règles précises concernant l'exécution des mandats. Deuxièmement, la Cour constate également que la création d'une règle générale voulant que les juges émetteurs doivent prévoir des protocoles de perquisition pourrait créer des difficultés pratiques. Il serait en effet difficile pour les juges de prédire quelle technique d'enquête devra être utilisée, notamment puisque les ordinateurs permettent de dissimuler de la preuve de plusieurs manières[383].

Malgré cette conclusion selon laquelle l'imposition d'un protocole de saisie ne sera généralement pas nécessaire, cela n'exclut pas la possibilité qu'elle le soit dans des cas très précis, tels qu'une fouille d'ordinateur « concernant des droits de propriété intellectuelle confidentiels ou encore des renseignements susceptibles d'être protégés par un privilège »[384]. Un protocole de saisie fut notamment imposé dans la décision *Ontario (Ministry of the Attorney General)* v. *Law Society of Upper Canada*, où l'ordinateur de travail d'un avocat de la défense a été saisi dans le cadre d'une enquête en matière de pornographie juvénile[385]. Certains auteurs soulignent que ce type de protocole pourrait également être pertinent lorsqu'un nombre élevé d'ordinateurs sont branchés en réseau, comme dans une entreprise multinationale, ou lorsque des tiers innocents sont visés par le mandat[386]. Par ailleurs, la Cour suprême a précisé que ses

---

[381] N. R. HASAN, préc., note 152, par. 70.
[382] *R.* c. *Vu*, préc., note 142, par. 55.
[383] *Id.*, par. 57.
[384] *Id.*, par. 62.
[385] *Ontario (Ministry of the Attorney General)* v. *Law Society of Upper Canada*, 2010 ONSC 2150.
[386] Gerald CHAN, « Life after Vu: Manner of Computer Searches and Search Protocols », (2014) 67-2 *S.C.L.R.* 433; N. R. HASAN, préc., note 152, par. 74.

conclusions sur le sujet sont appelées à changer, selon l'état des connaissances en matière de fouilles d'ordinateurs[387].

Toutefois, l'absence d'un protocole de saisie ne relève pas les policiers de leur obligation d'effectuer la fouille de manière raisonnable[388]. Dans la décision *Nurse and Plummer*, la Cour supérieure de l'Ontario a décidé que les policiers avaient agi de manière déraisonnable en examinant l'entièreté des données contenues dans des cellulaires saisis avec un mandat de perquisition[389]. Selon la Cour, la fouille des appareils aurait dû être limitée aux messages textes, au clavardage BBM[390], aux courriels, aux notes et au registre d'appels[391]. Pour cette raison, seuls ces éléments ont été admis en preuve.

Contrairement aux fouilles traditionnelles qui sont limitées dans le temps, les fouilles d'appareils électroniques n'ont pas cette contrainte temporelle. En effet, alors que le mandat de perquisition d'une résidence prévoit normalement une date d'exécution et une limite temporelle, le mandat de perquisition visant un appareil électronique ne prévoit normalement que cela : sa perquisition[392]. La saisie des données se trouvant dans l'appareil sera effectuée à une date ultérieure. L'analyse des données ainsi extraites peut prendre de nombreux jours, voir des semaines ou des mois. C'est ici que la distinction entre les termes disjonctifs « fouilles, saisies et perquisitions », qui se retrouvent à l'article 8 de la *Charte*, prend tout son sens dans le monde virtuel.

Cette particularité emporte une conséquence importante quant à l'étendue de la fouille d'appareils électroniques. En ayant plus de temps « sur les lieux de la perquisition », soit en l'espèce dans l'appareil électronique lui-même, les policiers ont un avantage important et peuvent fouiller plus en profondeur l'appareil. Cela peut parfois leur permettre de découvrir de

---

[387] *R.* c. *Vu*, préc., note 142, par. 62.
[388] *Id.*, par. 61.
[389] *R.* v. *Nurse and Plummer*, 2014 ONSC 5989, par. 24.
[390] BBM étant l'abréviation de BlackBerry Messenger. Voir WIKIPEDIA, « BlackBerry Messenger », dans Wikipedia, en ligne : <https://en.wikipedia.org/w/index.php?title=BlackBerry_Messenger&oldid=829127329> (consulté le 12 avril 2018).
[391] *R.* v. *Nurse and Plummer*, préc., note 389, par. 34.
[392] N. R. HASAN, préc., note 152, par. 57.

la preuve sur une autre infraction que celle sous enquête, soulevant ainsi la question de l'application de la théorie des « objets bien en vue » aux appareils électroniques.

Comme il a été décrit plus amplement ci-dessus, la doctrine des « objets bien en vue » permet aux policiers de saisir des objets qui ne sont pas spécifiés au mandat, dès lors que leur découverte est faite par inadvertance, que leur caractère illégal est apparent et que le policier se trouve légalement sur les lieux de la perquisition[393]. Dans un contexte informatique, l'application de cette théorie ne fait pas l'unanimité[394].

La décision *Jones*[395] de la Cour d'appel de l'Ontario est souvent citée lorsqu'il s'agit d'autoriser l'application de la théorie des « objets bien en vue » aux fouilles d'ordinateur. Dans ce dossier, les policiers enquêtaient sur une infraction de fraude et ont trouvé des éléments de preuve reliés à une autre infraction, soit l'infraction de possession de pornographie juvénile. Après la découverte de ces fichiers, ils ont continué leur fouille de l'ordinateur, à la recherche d'éléments de preuve sur cette seconde infraction, sans obtenir un nouveau mandat de perquisition. Ils ont ainsi accédé à des fichiers, en l'espèce des vidéos, qu'ils n'auraient normalement pas consultés lors d'une enquête pour fraude.

La Cour a d'abord conclu que l'étendue du mandat n'était pas trop large ; celui-ci était circonscrit à une fouille reliée à une fraude. Selon la Cour, un mandat de perquisition autorisant la fouille d'un appareil électronique n'est jamais une carte blanche pour les policiers, autorisant la fouille de l'appareil en entier. Les policiers doivent limiter leurs recherches à ce qui est pertinent pour leur enquête, telle que décrite dans le mandat de perquisition[396]. En ce qui concerne la théorie des « objets bien en vue », la Cour conclut qu'il est possible d'appliquer la théorie à la fouille d'appareils électroniques. Ainsi, la découverte par inadvertance d'éléments de preuve portant sur une infraction non prévue au mandat de perquisition ne serait pas contraire

---

[393] *R.* v. *Atkinson*, préc., note 178, par. 57.
[394] Voir notamment Aaron J. GOLD, « Obscured by Clouds: The Fourth Amendment and Searching Cloud Storage Accounts Through Locally Installed Software », (2015) 56 *William Mary Law Rev.* 2321, 2329-2331.
[395] *R.* v. *Jones*, 2011 ONCA 632.
[396] *Id.*, par. 42.

à l'article 8 de la *Charte*[397]. Or, une fois que le premier fichier de pornographie juvénile avait été trouvé, les policiers auraient dû obtenir un nouveau mandat de perquisition pour fouiller plus en profondeur l'appareil. À partir du moment où l'enquêteur cherchait de manière délibérée les éléments de pornographie juvénile et ouvrait des fichiers vidéo, qui n'étaient clairement pas pertinents dans le cadre de l'enquête de fraude, ni la théorie des « objets bien en vue », ni l'article 489 C.cr., ne pouvait autoriser la saisie[398].

La Cour d'appel du Québec, dans la décision *Boudreau-Fontaine*, traite également de la possibilité que la théorie des « objets bien en vue » permette la saisie des données liées à des infractions qui ne sont pas mentionnées au mandat de perquisition[399]. Dans ce cas, les policiers cherchaient dans l'ordinateur des éléments de preuve démontrant que l'accusé s'était connecté à Internet, ce qui lui était interdit dans le cadre d'une probation. En plus des éléments de preuve liés à la connexion à Internet, les policiers ont également découvert du matériel de pornographie juvénile. En l'espèce, la Cour souligne que :

> « la poursuite n'a présenté aucune preuve permettant de savoir si les agents étaient toujours dans le cadre de l'exécution du mandat lorsqu'ils ont découvert le matériel pornographique, donc qu'ils étaient toujours à la recherche des données démontrant que l'ordinateur était branché à Internet. Ainsi, rien n'établit que cette saisie s'est faite légalement ».[400]

Il est donc possible de conclure que la Cour d'appel du Québec est d'avis que la théorie des « objets bien en vue » peut s'appliquer en matière de fouilles informatiques, dans la mesure où les agents de l'État cherchent encore des éléments de preuve qui sont prévus au mandat et qu'ils découvrent par inadvertance des éléments de preuve portant sur une seconde infraction non mentionnée au mandat.

Dans un dossier quelque peu différent, la Cour supérieure de l'Ontario a également permis l'application de la théorie des « objets bien en vue » à la fouille d'un ordinateur. Dans la décision

---

[397] *Id.*, par. 64.
[398] *Id.*, par. 71; *R.* v. *Rafferty*, 2012 ONSC 703, par. 110.
[399] *R.* c. *Boudreau-Fontaine*, préc., note 186, par. 47 et suivants.
[400] *Id.*, par. 53.

R. v. *Mayo*[401], les policiers ont été appelés par un technicien informatique qui a aperçu deux fichiers portant un nom louche, lorsqu'il effectuait un travail de maintenance sur un ordinateur apporté par un client. Bien que l'ordinateur n'était plus ouvert lorsque les policiers sont arrivés sur place, la Cour a conclu que la théorie des « objets bien en vue » permettait au technicien de mettre l'appareil sous tension et de montrer les deux noms de fichiers aux policiers. Selon la Cour, les policiers auraient pu voir les noms de fichiers s'ils avaient été présents lorsque le technicien les avait découverts. Ainsi, la théorie des « objets bien en vue » permettait au technicien de retracer ses gestes et de montrer aux policiers comment il avait découvert les noms de fichiers[402].

Malgré l'existence de ces décisions qui autorisent l'application de la théorie des « objets bien en vue » à la fouille d'appareils électroniques, il existe également un courant jurisprudentiel et doctrinal à l'effet contraire. D'abord, dans la décision *Uber Canada inc.* c. *Agence du revenu du Québec*, le juge Cournoyer, en *obiter*, semble être d'avis que la seule solution possible au problème de la saisie de données non visées par le mandat soit « la création d'une règle qui interdit l'utilisation de la preuve qui n'est pas visée par un mandat de perquisition, car cette utilisation serait susceptible de rendre la manière d'effectuer la fouille abusive »[403]. Cette interprétation s'aligne avec l'opinion de plusieurs auteurs, notamment celle de Orin S. Kerr qui a opiné dès 2005 que l'abolition de la théorie des « objets bien en vue » pourrait éventuellement être la seule solution possible afin de réitérer l'importance et la fonction du Quatrième amendement américain[404], qui est l'équivalent de notre article 8 de la *Charte*. Selon lui, cette option s'impose maintenant en raison des avancées dans le monde informatique, notamment en raison de l'augmentation importante de la capacité de stockage de données des ordinateurs[405]. En fait, la solution serait simplement de proscrire l'utilisation de données qui sont reliées à des

---

[401] *R.* v. *Mayo*, 2016 ONSC 125.
[402] *Id.*, par. 33.
[403] *Uber Canada inc.* c. *Agence du revenu du Québec*, 2016 QCCS 2158, par. 284.
[404] O. S. KERR, préc., note 325, 577.
[405] Orin S. KERR, « Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data », (2015) 48 *Texas Tech Law Rev.* 1, 20.

infractions qui ne sont pas mentionnées au mandat de perquisition, sans même avoir à considérer l'application de la théorie des « objets bien en vue »[406].

Par ailleurs, selon Alan D. Gold, la théorie des « objets bien en vue » ne peut simplement pas s'appliquer en matière informatique puisque les policiers doivent poser un geste afin de découvrir la preuve. Contrairement aux perquisitions traditionnelles, où un policier peut simplement apercevoir un sachet de cannabis sur une table de chevet, les policiers doivent ouvrir les fichiers informatiques afin de découvrir leur caractère illégal. Ainsi, selon lui, la théorie ne peut simplement pas s'appliquer dans le monde virtuel[407].

Certains auteurs proposent plutôt une solution mitoyenne, à mi-chemin entre l'abolition complète et la reconnaissance pure et simple de la théorie des « objets bien en vue ». Par exemple, Lisa Jorgensen propose qu'une tierce partie effectue le triage des données recueillies dans les ordinateurs, afin de séparer les données pertinentes de celles susceptibles de révéler des détails non pertinents sur la vie de l'individu sous enquête[408]. Un auteur américain propose plutôt une solution se rapprochant de l'article 24(2) de la *Charte*. Selon Andrew Vahid Moshirnia, au lieu d'essayer de transposer la théorie des « objets bien en vue » à la fouille d'ordinateurs, nous devrions créer une nouvelle règle qui se concentrerait sur l'admissibilité *a posteriori* de la preuve[409]. Il s'agirait alors de balancer l'intérêt de la société à ce que le crime dévoilé soit puni et l'intérêt en matière de vie privée de l'individu sous enquête. Quoique cette proposition semble intéressante à première vue, nous pensons que celle-ci est inapplicable au Canada puisque ce genre d'analyse présuppose ici qu'il y a bel et bien eu violation de la *Charte*, alors que la théorie des « objets bien en vue » vient justement nier une telle violation. Par

---

[406] *Id.*, 11.
[407] A. D. GOLD, préc., note 264, par. 19; Voir aussi Larry E. DANIEL, « Plain View Doctrine in Digital Evidence Cases—A Common Sense Approach », *Forensic Magazine* (23 octobre 2009), en ligne : <https://www.forensicmag.com/article/2009/10/plain-view-doctrine-digital-evidence-cases%E2%80%94-common-sense-approach> (consulté le 13 avril 2018).
[408] L. JORGENSEN, préc., note 177, par. 42.
[409] Andrew Vahid MOSHIRNIA, « Separating Hard Fact from Hard Drive: A Solution for Plain View Doctrine in the Digital Domain », (2010) 23 *Harv. J. Law Technol.* 609, 626.

ailleurs, une incertitude serait créée pour les policiers qui ne pourraient pas savoir à l'avance si leur perquisition est légale ou non[410].

Bien qu'il serait surprenant que la Cour suprême abolisse éventuellement l'application de la théorie des « objets bien en vue » lors de la fouille d'ordinateurs, il serait néanmoins utile qu'elle se penche sur la question, afin de bien considérer les intérêts qui s'opposent.

[410] L'auteur lui-même souligne cette lacune, mais soutient que l'application répétée de cette règle créerait des précédents permettant une certaine prévisibilité. *Id.*, 627.

Chapitre 3 – La saisie de données sauvegardées dans le *nuage*

La manière par laquelle nous sauvegardons nos données personnelles a connu de grands changements dans les dernières années. Auparavant, si un individu voulait enregistrer un fichier informatique quelconque, il devait le faire sur un support physique qui lui appartenait, comme une disquette, un CD, un DVD, une clé USB ou un disque dur. Depuis 2006, lorsque l'entreprise Amazon a commencé à offrir son service AWS[411], cette réalité a bien changé[412]. Il est maintenant possible de sauvegarder nos données personnelles de manière délocalisée, c'est-à-dire sur des serveurs qui peuvent se trouver partout dans le monde, plutôt que dans nos propres appareils. Ce type de service – qui fait partir des diverses applications de l'infonuagique qui seront étudiées plus en détails ci-dessous – est de plus en plus populaire, notamment pour les entreprises[413].

Avant de considérer plus amplement les impacts juridiques de l'infonuagique, nous allons d'abord examiner le fonctionnement de cette nouvelle technologie, ses différentes applications et les défis que son utilisation soulève pour les forces de l'ordre. Nous expliquerons ensuite pourquoi, selon nous, les données sauvegardées de manière délocalisée peuvent tout de même bénéficier d'une attente raisonnable de vie privée et donc être protégées par l'article 8 de la *Charte*. Par la suite, nous analyserons divers scénarios susceptibles de se présenter pour les forces de l'ordre, afin de déterminer quel type d'autorisation judiciaire est applicable afin de permettre la saisie de ces données. Finalement, nous survolerons quelques considérations relatives aux juridictions, puisque les serveurs utilisés pour l'infonuagique peuvent se trouver partout dans le monde.

---

[411] AWS est un service d'infonuagique permettant notamment de sauvegarder des données à distance, sur un serveur appartenant à Amazon. AMAZON, « What is AWS? - Amazon Web Services », *Amazon Web Services, Inc.*, en ligne : <https://aws.amazon.com/what-is-aws/> (consulté le 30 avril 2018).

[412] L'infonuagique était appliqué avant cette date, mais le lancement du service d'Amazon nous permet de tracer une ligne à partir de laquelle l'utilisation de l'infonuagique a réellement pris de l'ampleur et où le terme a commencé à être plus répandu.

[413] BACKUPIFY, « Bits & Bytes: A History of Data Storage », en ligne : <https://www.backupify.com/history-of-data-storage/> (consulté le 30 avril 2018).

Section 3.1 Principes applicables à l'infonuagique

Il n'est pas nécessaire dans le cadre de ce mémoire d'examiner de manière très détaillée tous les aspects techniques reliés à l'infonuagique. Toutefois, certains principes de base doivent tout de même être expliqués.

3.1.1 La définition de l'infonuagique et ses différentes utilisations

Selon le *National Institute of Standards and Technology*, une agence du Département du commerce américain :

> « Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. […] »[414]

Le *nuage* est donc composé de ressources informatiques, accessibles par l'entremise d'un réseau, pouvant être employées pour plusieurs utilisations différentes, ou services différents. Certains auteurs accordent beaucoup d'importance à la distinction entre l'infonuagique (*cloud computing*) et les services offerts par l'entremise du *nuage* (*cloud services*)[415]. Toutefois, dans le cadre de ce mémoire, cette distinction est moins nécessaire[416]. Nous retiendrons donc que l'infonuagique se caractérise par le fait d'utiliser des applications et de sauvegarder des données sur un serveur distant, par l'entremise d'Internet, plutôt que sur nos propres appareils[417]. Les

---

[414] Peter MELL et Tim GRANCE, « The NIST Definition of Cloud Computing », *Computer security resource center*, en ligne : <https://csrc.nist.gov/publications/detail/sp/800-145/final> (consulté le 30 avril 2018).
[415] Josiah DYKSTRA et Damien RIEHL, « Forensic Collection of Electronic Evidence from Infrastructure-as-a-Service Cloud Computing », (2012) XIX-1 *Richmond J. Law Technol.* 1-47, 7.
[416] Si le lecteur est particulièrement intéressé par le fonctionnement de l'infonuagique, ses différentes utilisations et modèles, nous l'invitons à consuler Nicolas VERMEYS, Julie M. GAUTHIER et Sarit K. MIZRAHI, « Étude sur les incidences juridiques de l'utilisation de l'infonuagique par le gouvernement du Québec », en ligne : <https://www.vermeys.com/publications/etude-sur-les-incidences-juridiques-de-lutilisation-de-linfonuagique-par-le-gouvernement-du-quebec/> (consulté le 25 septembre 2018).
[417] William Jeremy ROBISON, « Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act », (2009) 98 *Georgetown Law J.* 1195, 1199; Matthew NIED, « Cloud Computing, the Internet, and the Charter Right to Privacy : the Effect of Terms of Service Agreements on Reasonable Expectations of Privacy », (2011) 69 *Advocate Vanc. Bar Assoc.* 701, 706.

utilisateurs ne sont alors pas propriétaires de la technologie qu'ils utilisent, mais plutôt locataires d'un espace virtuel fourni par une entreprise[418]. L'information ainsi sauvegardée sur le *nuage* peut être accédée à partir de n'importe quel appareil ayant une connexion Internet et les accès requis, à n'importe quel moment, à partir de n'importe où dans le monde[419].

Il y a trois principaux modèles de services d'infonuagique[420] : le SaaS (*Software as a Service* ou « logiciel en tant que service »), le PaaS (*Platform as a Service* ou « plate-forme en tant que service ») et le IaaS (*Infrastructure as a Service* ou « infrastructure en tant que service »)[421]. Le SaaS permet aux utilisateurs d'utiliser des applications à travers d'Internet, tel que des services de courriel en ligne[422]. Des exemples de ce modèle sont *Gmail* et *Hotmail*, de même que des logiciels de rédaction (*Office 365* et *Google Docs*), des logiciels de gestion des ventes (*Salesforce*) et des logiciels de gestion d'événements (*Planning Pod*)[423]. Le SaaS est également lié aux services de sauvegarde de données en ligne, tels que *Dropbox* ou *Microsoft OneDrive*[424]. L'utilisateur n'a pas le contrôle sur les applications utilisées et n'a pas à les télécharger ou à les tenir à jour; il ne fait qu'y accéder avec un nom d'utilisateur et un mot de passe[425]. Le SaaS est le type de *nuage* qui est le plus connu par les utilisateurs d'Internet[426], ce qui le rendra souvent le plus pertinent dans une enquête criminelle. Par ailleurs, un auteur souligne que l'utilisation

---

[418] Ilana R. KATTAN, « Cloudy Privacy Protections: Why the Stored Communications Act Fails to Protect the Privacy of Communications Stored in the Cloud », (2011) 13 *Vanderbilt J. Entertain. Technol. Law* 617, 621.
[419] Laurie BUCHAN SERAFINO, « "I Know My Rights, So You Go'n Need A Warrant for That": The Fourth Amendment, Riley's Impact, And Warrantless Searches of Third-Party Clouds », (2014) 19 *Berkeley J. Crim. Law* 154, 161.
[420] D'autres modèles sont disponibles et utilises par les entreprises, principalement dans le but de se distinguer de la competition. Voir N. VERMEYS, J. M. GAUTHIER et S. K. MIZRAHI, préc., note 416, 43.
[421] David S. BARNHILL, « Cloud Computing and Stored Communications: Another look at Quon v. Arch Wireless », (2010) 25 *Berkeley Technol. Law J.* 621-648. La traduction des termes est issue de WIKIPEDIA, « Cloud computing », dans Wikipédia, en ligne : <https://fr.wikipedia.org/w/index.php?title=Cloud_computing&oldid=147706181> (consulté le 30 avril 2018).
[422] D. S. BARNHILL, préc., note 421, 639.
[423] Gleb B., « Choosing the Right Cloud Service: IaaS, PaaS, or SaaS », *Ruby Garage*, en ligne : <https://rubygarage.org/blog/iaas-vs-paas-vs-saas> (consulté le 30 avril 2018).
[424] *Id.*
[425] *Id.*
[426] D. S. BARNHILL, préc., note 421, 639.

de ce type de service n'est pas sans risque puisque l'utilisateur ne sait pas où se trouvent ses données, ce qui diminue son contrôle sur celles-ci[427].

Le PaaS donne plus de possibilités aux usagers. Le fournisseur de ce type de service va créer une plateforme pour que les utilisateurs puissent créer leurs propres applications. Il va également fournir l'infrastructure de la plateforme, de sorte que les usagers n'aient pas à entretenir l'infrastructure (tels que les serveurs eux-mêmes ou encore le logiciel d'exploitation)[428]. Il s'agit donc d'un modèle idéal pour les entreprises ou les particuliers qui développent des applications[429]. Ce modèle est facilement adaptable aux besoins grandissants d'une entreprise; il est facile d'augmenter la taille du *nuage* ou de modifier les paramètres de celui-ci au rythme de l'évolution de l'entreprise[430]. Toutefois, un risque est également présent puisque ce modèle cause une dépendance importante entre le client et le fournisseur de service. Ainsi, si le fournisseur décidait de changer ses paramètres ou s'il était contraint de fermer pour des motifs financiers, le client pourrait se trouver dans une situation fâcheuse[431].

Finalement, avec le modèle IaaS, seule l'infrastructure est fournie. Le fournisseur de service s'occupe donc des installations physiques où se trouvent les serveurs, ainsi que l'accessibilité à ceux-ci[432]. L'utilisateur peut donc moduler comme bon lui semble l'infrastructure, en y installant tout ce qu'il désire[433]. Il s'agit surtout d'un modèle pertinent pour les entreprises[434].

Ces trois modèles peuvent être conceptualisés comme une pyramide : à la base se trouve le IaaS, où l'usager a un contrôle total du contenu et de la structure de son *nuage*; au milieu se trouve le PaaS, où l'usager a un contrôle partiel du contenu et de la structure, mais où la facilité d'utilisation est plus grande; et finalement à la pointe se trouve le SaaS, où l'usager n'a aucun

---

[427] Timothy D. MARTIN, « Hey! You! Get Off of My Cloud: Defining and Protecting the Metes and Bounds of Privacy, Security and Property in Cloud Computing », (2010) 92 *J. Pat. Trademark Off. Soc.* 283, 289.
[428] D. S. BARNHILL, préc., note 421, 639-640.
[429] G. B., préc., note 423.
[430] T. D. MARTIN, préc., note 427, 291.
[431] *Id.*
[432] APPRENDA, « IaaS, PaaS, SaaS (Explained and Compared) », *Apprenda*, en ligne : <https://apprenda.com/library/paas/iaas-paas-saas-explained-compared/> (consulté le 30 avril 2018).
[433] D. S. BARNHILL, préc., note 421, 640.
[434] G. B., préc., note 423.

contrôle, mais il bénéficie d'une facilité d'utilisation importante pour les services fournis par le fournisseur de service[435]. L'analogie de la pyramide permet également de comprendre les différentes composantes du *nuage*, soit l'infrastructure, la plate-forme et les logiciels. L'infrastructure est à la base du *nuage*, il s'agit du réseau lui-même, des ordinateurs, des serveurs et des outils de sauvegarde des données qui se trouvent physiquement chez le fournisseur de service[436]. La plate-forme est ce qui permet d'utiliser l'infrastructure, comme le système d'exploitation[437] de nos ordinateurs personnels. Finalement, les logiciels (ou applications) permettent d'utiliser la plate-forme pour une utilisation particulière, telle que les courriels.

Bien qu'il soit possible pour une entreprise de créer ses propres installations d'infonuagique, évitant ainsi de passer par un fournisseur de service, cette façon de faire est assez rare considérant les ressources importantes nécessaires à un tel projet. En effet, l'entreprise serait alors responsable de l'entretien de l'infrastructure de son *nuage*, incluant le remplacement physique des serveurs, lorsque nécessaire[438]. Il existe toutefois une autre façon d'avoir un *nuage privé* (ou *private cloud* en anglais), sans avoir à investir dans l'infrastructure nécessaire à l'ouverture d'un centre de données privé. Certains fournisseurs de service d'infonuagique offrent la possibilité d'avoir un serveur dédié entièrement à un seul et unique client, créant donc l'équivalent d'un *nuage* qui serait situé sur les lieux d'affaires de l'entreprise[439]. Dans les deux cas, malgré des coûts plus importants, le *nuage privé* confère à l'entreprise une plus grande sécurité envers ses données[440].

Cependant, dans la majorité des cas, le *nuage* sera plutôt *public*, c'est-à-dire que l'infrastructure du *nuage* sera partagée par tous les utilisateurs, qui ne peuvent toutefois qu'accéder à leurs

---

[435] *Id.*
[436] WIKIPEDIA, « Infrastructure as a service », dans Wikipédia, en ligne : <https://fr.wikipedia.org/w/index.php?title=Infrastructure_as_a_service&oldid=143431424> (consulté le 30 avril 2018).
[437] *Operating system* (ou *OS*) en anglais.
[438] John WHITE, « Private vs. Public Cloud: What's the Difference? », *Expedient* (5 juin 2014), en ligne : <https://www.expedient.com/blog/private-vs-public-cloud-whats-difference/> (consulté le 30 avril 2018).
[439] MICROSOFT, « Public Cloud vs Private Cloud vs Hybrid Cloud », *Microsoft Azure*, en ligne : <https://azure.microsoft.com/en-gb/overview/what-are-private-public-hybrid-clouds/> (consulté le 30 avril 2018).
[440] J. WHITE, préc., note 438.

propres données[441]. Le *nuage public* a l'avantage d'être moins coûteux qu'un *nuage privé*, tout en fournissant une sécurité contre la perte de données puisque celles-ci peuvent être réparties sur plusieurs serveurs différents, plutôt que sur un seul[442]. Un service de *nuage hybride* peut également être utilisé, offrant plus de possibilités aux entreprises choisissant cette option[443].

3.1.2 La croissance de cette pratique dans le monde

Plusieurs avantages peuvent être reliés à l'infonuagique, expliquant sa croissance rapide. Tout d'abord, lorsqu'il est question de SaaS, l'un des avantages est que l'utilisateur n'a pas à télécharger ou mettre à jour ses applications, ce qui facilite l'utilisation et peut faire gagner du temps aux usagers[444]. Par ailleurs, plusieurs applications utilisant les services d'infonuagique sont gratuites, facilement accessibles pour les usagers et permettent l'accès aux données à partir de n'importe quel appareil[445]. De plus, si l'appareil utilisé pour accéder au *nuage* fait défaut, les données ne sont pas affectées et demeurent accessibles puisque celles-ci ne sont pas directement sur l'appareil, mais sur des serveurs distants[446]. En fait, les données sont habituellement situées sur plusieurs serveurs séparés, afin d'assurer l'accès aux données si un serveur faisait défaut[447]. La réduction des coûts de gestion est également un avantage important relié à l'utilisation de l'infonuagique pour les entreprises[448]. Le gouvernement américain, qui s'est doté d'une politique privilégiant l'utilisation du *nuage*[449], reconnaît quatre avantages principaux reliés à l'utilisation du *nuage* :

> « (1) improving service delivery to internal and external customers; (2) introducing scalability, on demand provisioning, and resource pooling; (3) enhancing collaboration

---

[441] MICROSOFT, préc., note 439.
[442] *Id.*
[443] *Id.*
[444] APPRENDA, préc., note 432.
[445] D. S. BARNHILL, préc., note 421, 641.
[446] IBM, « IaaS PaaS SaaS Cloud Service Models », *IBM*, en ligne : <https://www.ibm.com/cloud/learn/iaas-paas-saas> (consulté le 30 avril 2018).
[447] Sarit K. MIZRAHI, « The Dangers of Sharing Cloud Storage: The Privacy Violations Suffered by Innocent Cloud Users during the Course of Criminal Investigations in Canada and the United States », (2017) 25 *Tulane J. Int. Comp. Law* 303, 308.
[448] D. S. BARNHILL, préc., note 421, 641.
[449] U.S. DEPARTMENT OF THE INTERIOR, « The Cloud First Strategy » (23 août 2017), en ligne : <https://www.doi.gov/cloud/strategy> (consulté le 10 mai 2018).

> within each agency; and (4) replacing legacy IT infrastructure that is at the end of its lifespan. »[450]

De nombreux utilisateurs du *nuage* le font sans même le savoir[451]. En effet, l'interface de certains services fait en sorte que les usagers ne réalisent pas qu'ils utilisent l'infonuagique. On peut penser notamment à *Facebook* et à *LinkedIn*, deux sites de réseautage qui utilisent le *nuage* afin de sauvegarder les diverses informations qu'un usager partage sur sa page personnelle[452].

L'infonuagique est théoriquement sans limites, au sens où tout ce qui peut être effectué de manière locale sur notre propre appareil peut également être exécuté de manière délocalisée sur le *nuage*[453]. Pour cette raison,

> « users are switching to cloud computing because it provides the same traditional type of networking and file storage capacities for a fraction of the price. In fact, individuals and businesses alike are buying cheaper and less sophisticated machines because large hard drives are no longer necessary; users can stream programs such as word processing or online gaming, directly from the cloud. »[454]

Statistiquement parlant, la croissance du *nuage* n'est plus à prouver. Depuis 2009, les dépenses liées à l'infonuagique ont augmenté 4.5 fois plus rapidement que les dépenses générales en technologies de l'information[455]. Le nombre d'utilisateurs de l'infonuagique serait passé de 2.4 milliards en 2013 à 3.6 milliards en 2018[456]. Selon l'*Institut de la statistique* du Québec, le

---

[450] Dena G. MCCORRY, « With Cloud Technology, Who Owns Your Data? », (2014) 8 *Fed. Courts Law Rev.* 125, 130.
[451] Quinn HOCHHALTER, « The Sky's the Limit: Twenty-First Century Searches of Hard-Drives, Smartphone Applications, & the Cloud », (2014) 90 *N. D. Law Rev.* 171, 178.
[452] D. G. MCCORRY, préc., note 450, 129.
[453] Nicolette LOTRIONTE, « The Sky's the Limit - The Border Search Doctrine and Cloud Computing », (2013) 78 *Brooklyn Law Rev.* 663, 680.
[454] Sara J. KOHLS, « Searching the Clouds - Why Law Enforcement Officials Need to Get Their Heads Out of the Cloud and Obtain a Warrant Before Accessing a Cloud Network Account », (2012) 4 *Case West. Reserve J. Law Technol. Internet* 169, 173.
[455] L. COLUMBUS, préc., note 14.
[456] STATISTA, « Consumer cloud computing user worldwide 2018 », *Statista*, en ligne : <https://www.statista.com/statistics/321215/global-consumer-cloud-computing-users/> (consulté le 9 mai 2018).

nombre d'entreprises branchées qui utilisent l'infonuagique au Québec a cru de manière appréciable entre 2012 et 2016[457].

3.1.3 Les défis posés par l'infonuagique pour les forces de l'ordre

Dans la culture populaire, on entend souvent que le *nuage* n'existe pas réellement, qu'il ne s'agit que de l'ordinateur de quelqu'un d'autre[458]. Cette particularité du *nuage* est justement ce qui cause tant de fil à retordre aux forces de l'ordre. En effet, auparavant, si les policiers cherchaient de l'information concernant un suspect en particulier, ils pouvaient s'attendre à ce que les données contenues dans son ordinateur personnel soient pertinentes. Or, maintenant, les données pertinentes à une enquête criminelle peuvent se trouver partout dans le monde, sur des serveurs n'appartenant pas à l'individu sous enquête[459]. La multiplication des endroits où les policiers sont susceptibles de trouver de l'information pertinente à leur enquête complique bien évidemment celle-ci.

Pour aggraver davantage la situation, il arrivera souvent que les policiers ignorent si un suspect utilise des services d'infonuagique. Ils pourront parfois le découvrir lors d'une saisie visant l'ordinateur du suspect, mais cela ne sera pas toujours le cas. Des experts en informatique devront donc effectuer des recherches approfondies, par exemple en demandant à plusieurs fournisseurs de service s'ils hébergent des données liées à une adresse IP particulière[460]. Certaines traces laissées sur les appareils électroniques des usagers du *nuage* peuvent également permettre de déterminer quel FSI est utilisé par un individu et où se trouvent les données de l'individu sur le *nuage* de l'entreprise en question[461].

---

[457] INSTITUT DE LA STATISTIQUE DU QUÉBEC, « Part des entreprises branchées qui utilisent l'infonuagique, Québec, 2012 et 2016 », en ligne : <http://www.stat.gouv.qc.ca/statistiques/science-technologie-innovation/utilisation-internet/entreprises/utilisation-infonuagique.html> (consulté le 9 mai 2018).
[458] « *There is no cloud, it's just someone else's computer*. » Auteur inconnu.
[459] Daniel M. SCANLAN, « Issues in digital evidence and privacy: Enhanced expectations of privacy and appellate lag times », (2012) 16 *Can. Crim. Law Rev.* 301, 311.
[460] Le fournisseur de service serait effectivement en mesure de retracer l'adresse IP utilisée afin de se connecter à ses services. J. DYKSTRA et D. RIEHL, préc., note 415, 22.
[461] S. K. MIZRAHI, préc., note 447, 312.

Qui plus est, même une fois les données recueillies par les policiers, leur analyse est susceptible d'être plus compliquée que si les données avaient été trouvées sur l'ordinateur physique du suspect. En effet, « by their nature, cloud-computing environments are more complex than a single computer or a server »[462]. Ainsi, un technicien spécialisé en informatique devra vraisemblablement passer plus de temps à analyser les données obtenues, afin de trouver celles qui sont pertinentes à l'enquête.

Bref, la mobilité des données des individus pose problème pour les forces de l'ordre qui veulent trouver des éléments de preuve sur des appareils électroniques[463]. Par ailleurs, comme il sera étudié plus amplement à la section 3.5 du présent mémoire, la question de la juridiction applicable est également susceptible de compliquer le travail des policiers.

Section 3.2 L'attente de vie privée envers les données sauvegardées dans le *nuage*

L'existence même d'une attente raisonnable de vie privée concernant les données sauvegardées dans le *nuage* se pose. En effet, les données sauvegardées par l'entremise de services d'infonuagique sont souvent partagées avec un tiers et elles se situent dans un endroit où l'accusé n'a pas de contrôle, ce qui peut influencer l'attente de vie privée[464]. Ce débat est très important aux États-Unis où plusieurs auteurs s'opposent à l'application de la *third-party doctrine*, qui nie l'existence d'une attente raisonnable de vie privée dès que les informations sont partagées avec un tiers.

Ce problème n'a pas été traité en profondeur au Canada, mais nous croyons que la dissidence dans la décision *Cole* donne un indice à l'effet que ces données bénéficient également d'une attente raisonnable de vie privée. Selon celle-ci, « comme plus de données sont stockées dans le *nuage* et qu'on y a accès tant sur l'ordinateur de travail que l'ordinateur personnel, la propriété

[462] J. DYKSTRA et D. RIEHL, préc., note 415, 38.
[463] S. J. KOHLS, préc., note 454, 169.
[464] *R.* c. *Edwards*, préc., note 89, par. 45.

de l'appareil ou des données, loin de constituer un critère déterminant de l'attente raisonnable en matière de protection de la vie privée, devient un repère de plus en plus inutile. »[465]

Dans cette section, nous traiterons premièrement de cette approche américaine qui nie l'existence d'une attente raisonnable de vie privée envers les données délocalisées, qui sont sous le contrôle d'un tiers. Ultimement, nous démontrerons pourquoi celle-ci ne peut s'appliquer au Canada. Ensuite, nous examinerons certains facteurs pertinents dans la détermination d'une attente de vie privée, qui sont spécifiques aux données situées dans le *nuage*. Finalement, nous exposerons les motifs permettant de conclure qu'une telle attente de vie privée existe et que les données délocalisées sont donc protégées par l'article 8 de la *Charte*.

3.2.1 L'approche américaine

La *third-party doctrine* a été établi par les tribunaux américains dans un contexte de fouilles, saisies et perquisitions traditionnelles, c'est-à-dire qui ne portent pas sur du matériel informatique[466]. Selon cette doctrine, dès qu'un individu divulgue de l'information à une tierce partie, cette information ne peut plus faire l'objet d'une attente raisonnable de vie privée[467]. Donc, lorsque le tiers remet cette information aux forces de l'ordre, il ne s'agit pas d'une fouille, au sens de la célèbre décision *Katz*[468]. Cette négation du droit à la protection contre les fouilles, perquisitions ou saisies abusives serait justifiée par le risque que ce tiers divulgue l'information recueillie[469].

Plus récemment, cette doctrine a été utilisée par les tribunaux américains afin de nier l'existence d'une attente raisonnable de vie privée envers des données informatiques détenues par des entreprises, portant sur leurs clients[470]. L'application de cette théorie aux nouvelles technologies

---

[465] *R.* c. *Cole*, préc., note 94, par. 109.
[466] *United States* v. *Miller*, 423 U.S. 435, 443 (1976); *Smith* v. *Maryland*, 422 U.S. 735, 743-44 (1979); *Hoffa* v. *United States*, 385 U.S. 293 (1966); *Couch* v. *United States*, 409 U.S. 322 (1973).
[467] Q. HOCHHALTER, préc., note 451, 180.
[468] *Katz* v. *United States*, 389 U.S. 347 (1967).
[469] L. BUCHAN SERAFINO, préc., note 419, 156.
[470] *Id.*, 168 citant les décisions *United States* v. *Skinner*, 690 F.3d 772; *United States* v. *Lifshitz*, 369 F.3d 173; *United States* v. *Rigmaiden*, No. CR 08-814-PHX-DGC, 2013 QL 1932800; *United States* v. *Wilson*, No. 1:11-CR-53-TCB-ECS-3, 2012 WL 1129199; *United States* v. *Madison*, No. 11-60285-CR, 2012 WL 3095357; *In re*

est toutefois vivement critiquée par certains auteurs américains, qui militent plutôt pour la reconnaissance d'une attente raisonnable de vie privée visant les données personnelles, et ce, peu importe leur emplacement géographique[471]. Selon ceux-ci, dans un contexte d'infonuagique, la *third-party doctrine* ne devrait pas permettre aux forces de l'ordre d'obtenir lesdites données sans l'obtention préalable d'une autorisation judiciaire appropriée, puisque le fournisseur de service ne fait qu'emmagasiner les données d'un tiers[472]. En ce sens, les fournisseurs de service ne sont que des « mere custodians of the data, […] ensuring that data is neither lost nor damaged »[473]. Ainsi, tout comme une conversation téléphonique est protégée bien qu'elle ait lieu sur le réseau d'une entreprise, le contenu du *nuage* devrait être protégé[474]. Ce raisonnement est toutefois sujet aux conditions de service imposées par les FSI qui peuvent prévoir un accès et une utilisation des données par ces derniers, ce qui sera étudié plus en détail ci-dessous.

Selon ces auteurs, la doctrine devrait également être écartée pour le motif que le fournisseur de service d'infonuagique n'a pas à consulter les données de ses clients afin d'effectuer la sauvegarde; le processus s'effectuant plutôt de manière automatisée, par un système informatique. Ainsi, en l'absence d'intervention humaine, on ne peut affirmer que l'attente de vie privée des gens est diminuée ou anéantie[475]. Les données ne seraient donc pas réellement divulguées à une tierce partie[476]. Toutefois, il importe de rappeler qu'il a été révélé par Edwards Snowden que plusieurs FSI accédaient aux données de leurs client et les communiquaient au gouvernement américain dans le cadre du programme PRISM[477]. Ainsi, cet argument peut

---

Application of United States for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013); *United States* v. *Graham*, 846 F. Supp. 2d 384, 389 (D. Md. 2012); *In re* Application of the U.S. for an Order Pursuant to 18 U.S.C. s. 2703, 830 F. Supp. 2d 114, 133 (E.D. Va. 2011). .

[471] La position inverse semble effectivement minoritaire. À ce sujet, voir principalement Orin S. KERR, « The Case for the Third-Party Doctrine », (2009) 107 *Mich. Law Rev.* 561.

[472] L. BUCHAN SERAFINO, préc., note 419, 171.

[473] A. J. GOLD, préc., note 394, 2341.

[474] N. LOTRIONTE, préc., note 453, 687.

[475] O. S. KERR, préc., note 285, 1038; Andrew J. PECORARO, « Drawing Lines in the Cloud: Implications of Extraterritorial Limits to the Stored Communications Act », (2017) 51 *Creighton Law Rev.* 75, 103.

[476] Wei Chen LIN, « Where Are Your Papers: The Fourth Amendment, the Stored Communications Act, the Third-Party Doctrine, the Cloud and Encryption », (2016) 65 *DePaul Law Rev.* 1093, 1114.

[477] Lavanya RATHNAM, « PRISM, Snowden and Government Surveillance: 6 Things You Need to Know », *Cloudwards* (29 mars 2017), en ligne : <https://www.cloudwards.net/prism-snowden-and-government-surveillance/> (consulté le 25 septembre 2018).

sembler utopiste ou peut-être naïf. Par ailleurs, le fait que les usagers n'aient plus réellement le choix de recourir à l'infonuagique – en raison de la prévalence de cette technologie et du caractère désuet de ses alternatives – serait également un argument militant pour l'abolition de la *third-party doctrine* dans un contexte d'infonuagique[478], de même que la constatation que les données situées dans le *nuage* sont de nature privée, non pas publique[479].

Selon Neil Richards, l'application de la *doctrine* au *nuage* met tout simplement la protection constitutionnelle contre les fouilles, saisies et perquisitions abusives et le droit à la vie privée à risque :

> « The broad reading of the Third-Party Doctrine puts the Fourth Amendment at risk. For centuries, our criminal justice system has limited the power of the state by presuming not only that one is innocent until proven guilty but also that one has the right to be free of police monitoring and interference unless there is probable cause to suspect that one has committed a crime. The warrant requirement forces police to persuade a judge that an individual is up to no good. It can be inconvenient, which is precisely the point. But if our data – the facts or our lives – are no longer locked up in secure analog technologies and are also unprotected by the warrant requirement, surveillance and interference becomes much easier, and the specter of a police state looms large. It undermines not just our privacy but indeed any claim that we live in a free society. »[480]

Une autre approche a été proposée afin de réconcilier la *third-party doctrine* et la protection qui devrait être offerte aux données sauvegardées dans le *nuage*. Selon un auteur, il s'agirait simplement de reconnaître un privilège à ces données, de la même manière qu'un privilège protège les communications privilégiées entre un avocat et son client[481].

Au Canada, considérant la décision *Duarte* et le rejet de l'analyse fondée sur le risque[482], ainsi que les nombreuses décisions où les informations détenues en mains tierces se sont vu accorder la protection de l'article 8 de la *Charte*[483], il est clair que le partage des données avec un tiers

---

[478] L. BUCHAN SERAFINO, préc., note 419, 172; W. C. LIN, préc., note 473, 1114.
[479] L. BUCHAN SERAFINO, préc., note 419, 177.
[480] Neil RICHARDS, « The Third-Party Doctrine and the Future of the Cloud », (2017) 94 *Wash. Univ. Law Rev.* 1441, 1485.
[481] J. M. SMALL, préc., note 15.
[482] *R.* c. *Duarte*, préc., note 10.
[483] Nous pensons notamment aux décisions *R.* c. *Spencer*, préc., note 94; *R.* c. *Société TELUS Communications*, préc., note 195.

ne peut justifier d'écarter complètement la protection constitutionnelle contre les fouilles, saisies et perquisitions abusives[484]. Cet élément a d'ailleurs été repris récemment dans la décision *Marakah*, où la majorité a rappelé que

> « [l]a jurisprudence est claire : une personne ne perd par le contrôle de renseignements pour l'application de l'art. 8 uniquement parce que quelqu'un d'autre les possède ou peut les consulter. Même lorsque "la réalité technologique" (*Cole*, par. 54) l'empêche d'exercer un contrôle exclusif sur ses renseignements personnels, une personne peut malgré tout s'attendre raisonnablement à ce que ces renseignements soient à l'abri du regard scrutateur de l'État. »[485]

Ce seul critère ne serait donc pas suffisant afin de nier l'existence d'une attente raisonnable de vie privée, puisqu'une analyse contextuelle doit être effectuée afin de déterminer s'il y a attente raisonnable de vie privée. La doctrine américaine sur la question demeure toutefois pertinente puisque l'analyse fondée sur le Quatrième amendement américain est très similaire à celle fondée sur l'article 8 de la *Charte* ; les deux s'appuyant sur l'existence d'une attente raisonnable de vie privée afin que la protection soit enclenchée. Il faudra donc considérer d'autres éléments, tels que les conditions de service qui sont imposées par les FSI, ainsi que les lois portant sur la protection des renseignements personnels, afin de déterminer si les données sauvegardées dans le *nuage* peuvent être protégées par l'article 8 de la *Charte*.

3.2.2 L'impact des conditions de service imposées par les FSI et des lois portant sur la protection des renseignements personnels

En première instance dans la décision *Spencer*, le juge avait déterminé que l'attente de vie privée de l'accusé ne pouvait être considérée comme raisonnable en raison des dispositions contractuelles et législatives applicables, ce qui avait également été retenu en appel[486]. Toutefois, la Cour suprême en est plutôt arrivée à une conclusion différente. Selon la Cour, « les cadres législatifs et contractuels peuvent être pertinents, mais pas nécessairement déterminants,

---

[484] *R.* v. *Craig*, 2016 BCCA 154, par. 105 et suivants.
[485] *R.* c. *Marakah*, préc., note 81, par. 41.
[486] *R.* c. *Spencer*, préc., note 93, par. 52; Pour un portrait de la situation sur cette question avant la décision de la Cour suprême dans *Spencer*, voir également M. NIED, préc., note 417, 702.

quant à la question de savoir s'il existe une attente raisonnable de vie privée »[487]. La Cour en est venue à cette conclusion en citant la décision *Gomboc*, où il avait été déterminé que le contrat entre un fournisseur de services et son client était d'une grande importance, mais qu'il n'était qu'un des facteurs pertinents à l'analyse[488].

Aucune loi canadienne ne s'applique spécifiquement aux données situées dans le *nuage*. La *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) semble toutefois bel et bien s'appliquer en matière d'infonuagique[489]. Ainsi, les entreprises d'infonuagique devront normalement obtenir le consentement du client avant de divulguer des renseignements personnels[490], sous réserve des conditions de services imposées par les FSI, ce qui sera examiné ci-après. Certaines exceptions existent toutefois, notamment dans le cadre d'enquêtes criminelles[491]. Toutefois, tel que noté dans la décision *Spencer*, « les dispositions de la LPRPDE ne sont pas très utiles pour déterminer s'il existe une attente raisonnable en matière de vie privée puisqu'après les avoir examinées, on se retrouve au point de départ. »[492] Ces dispositions sont donc d'un intérêt assez limité lorsque nous sommes à l'étape de déterminer s'il y a attente raisonnable de vie privée envers les données du *nuage*.

Aux États-Unis, les FSI ont une obligation de faire rapport aux autorités lorsqu'ils savent qu'un client a sauvegardé des fichiers de pornographie juvénile sur son *nuage*[493]. Une obligation similaire est prévue au Canada, en vertu de la *Loi concernant la déclaration obligatoire de la pornographie juvénile sur Internet par les personnes qui fournissent des services Internet*[494]. Afin de respecter cette obligation, plusieurs FSI, notamment *Microsoft*, *Facebook* et *Twitter*, ont mis sur place un programme permettant d'identifier de telles photos de manière automatique, dès que les photos sont sauvegardées sur le *nuage*[495]. Les FSI peuvent ensuite aviser les autorités

---

[487] *R.* c. *Spencer*, préc., note 94, par. 54.
[488] *R.* c. *Gomboc*, préc., note 24, par. 31-32.
[489] *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, c. 5, art. 4(1)a).
[490] *Id.*, part. Annexe 1, article 4.3.
[491] *Id.*, art. 7.
[492] *R.* c. *Spencer*, préc., note 94, par. 61.
[493] *Victims of Child Abuse Act*, (1990), U.S. Code, Title 18 – Crimes and Criminal Procedure, Chapter 110.
[494] *Loi concernant la déclaration obligatoire de la pornographie juvénile sur Internet par les personnes qui fournissent des services Internet*, L.C. 2011, c. 4.
[495] *R.* v. *Cusick*, 2015 ONSC 6739, par. 14.

pour que celles-ci obtiennent un mandat de perquisition visant les appareils électroniques du suspect. Lorsqu'une entreprise américaine identifie une adresse IP canadienne qui aurait été utilisée afin de sauvegarder de telles données dans le *nuage*, le FSI va contacter la *Gendarmerie Royale du Canada* (GRC) afin que l'enquête se poursuive de notre côté de la frontière[496].

Dans la décision *Cusick*, les autorités canadiennes se sont basées sur un tel rapport fait par un FSI américain afin d'obtenir un mandat de perquisition visant un ordinateur situé au Canada[497]. Bien qu'ultimement un nouveau procès ait été ordonné, la Cour supérieure de l'Ontario a conclu que le rapport fourni par le FSI était une source crédible pouvant être utilisée par les autorités canadiennes afin d'obtenir un mandat de perquisition, sans que cette information n'ait besoin d'être autrement vérifiée[498].

Bien que démontrant que les FSI peuvent accéder aux données de leurs clients, nous pensons que ces obligations de divulgation ne font pas obstacle à la reconnaissance d'une attente raisonnable de vie privée envers les données du *nuage*. Comme la décision *Cusick* le démontre, les FSI vont principalement utiliser des logiciels automatisés afin d'identifier les fichiers de pornographie juvénile. Cela veut donc dire que les fichiers déposés sur le *nuage* ne sont pas examinés individuellement par un employé du FSI. Ainsi, les données demeurent pour la plupart confidentielles et non consultées par les FSI.

Outre les lois générales s'appliquant en matière de vie privée, la relation entre un FSI et un client est également régie par des conditions de service (*terms of service*) et par des politiques concernant la vie privée (*privacy policy*). Les conditions de service imposées[499] par un FSI peuvent varier grandement, notamment en ce qui concerne l'accès aux données des clients. Certaines entreprises, telles que *Mozy* et *SpiderOak*, prévoient dans leurs conditions de service

---

[496] *Id.*, par. 23.
[497] *Id.*, par. 35.
[498] *Id.*, par. 94.
[499] Les conditions de service sont effectivement non-négociables entre le FSI et le client et elles favorisent le FSI. Voir Jay P. KESAN, Carol M. HAYES et Masooda N. BASHIR, « Information Privacy and Data Control in Cloud Computing: Consumers, Privacy Preferences, and Market Efficiency », (2013) 70 *Wash. Lee Law Rev.* 341, 421.

qu'elles n'accéderont pas aux données sauvegardées sur le *nuage* de leurs clients[500]. Plus encore, ces entreprises ont mis en place des systèmes de cryptage sophistiqué qui font en sorte qu'elles ne sont même pas en mesure d'accéder aux données de leurs clients[501]. À l'autre extrémité du spectre, certains FSI indiquent dans leurs conditions qu'ils peuvent consulter les données de leurs clients à leur guise, sans aucun motif. C'est notamment le cas de *Apple*, de *Google* et de *DropBox*[502]. *Apple* spécifie toutefois dans ses politiques de confidentialité qu'elle ne fournira jamais aux forces de l'ordre les clés de cryptage des données utilisées par ses clients[503], tandis que *DropBox* crypte ses données, mais ne mentionne pas si elle pourrait éventuellement remettre les clés de cryptage aux autorités[504]. Certains FSI, tel que *Microsoft*[505], indiquent plutôt qu'ils n'accéderont pas aux données de leurs clients, sauf dans le cadre d'une enquête interne sur la violation des conditions d'utilisation applicables. Pour sa part, *Amazon* indique qu'elle accédera aux données de ses clients seulement à la demande d'une autorité gouvernementale, ou afin d'exécuter sa prestation de services[506].

En ce qui concerne le partage des données avec les autorités, il y a également plusieurs différences dans les ententes de confidentialité applicables :

> « […] Essentially, while some will only do so where the release of user information is appropriate or reasonably appropriate, others will rely on a "good-faith belief" that it is either necessary, reasonably necessary, or appropriate.

---

[500] MOZY, « Privacy Statement », en ligne : <https://mozy.com/about/legal/privacy> (consulté le 15 mai 2018); SPIDEROAK, « Privacy Policy », *SpiderOak*, en ligne : <https://spideroak.com/privacy-policy/> (consulté le 15 mai 2018).

[501] MOZY, « Online Backup Storage and Software for photos, music, and docs », en ligne : <https://mozy.com/product/mozy/personal> (consulté le 15 mai 2018); SPIDEROAK, « No Knowledge, Secure-by-Default Products », en ligne : <https://spideroak.com/no-knowledge/> (consulté le 15 mai 2018).

[502] GOOGLE, « Terms of Service – Privacy & Terms », en ligne : <https://policies.google.com/terms> (consulté le 15 mai 2018); APPLE, « iCloud Terms and Conditions », *Apple Legal*, en ligne : <https://www.apple.com/legal/internet-services/icloud/en/terms.html> (consulté le 15 mai 2018); DROPBOX, « Terms », *Dropbox*, en ligne : <https://www.dropbox.com/privacy> (consulté le 15 mai 2018).

[503] S. K. MIZRAHI, préc., note 447, 312.

[504] *Id.*, 311.

[505] MICROSOFT, « Services Agreement », en ligne : <https://www.microsoft.com/en-ca/servicesagreement/> (consulté le 15 mai 2018).

[506] AMAZON, « AWS Customer Agreement », *Amazon Web Services, Inc.*, en ligne : <https://aws.amazon.com/agreement/> (consulté le 15 mai 2018); DROPBOX, préc., note 502.

> The privacy policies also specify a host of reasons that dictate the necessity of disclosing the information of its users, namely for the purposes of: complying with the law, regulation, and legal processes; preventing fraud; protecting property rights; protecting others from death or serious bodily injury; maintaining the security of their system; or enforcing their terms of service agreements. It is noteworthy, however, that both Google and Microsoft specify that their disclosure of user data to comply with the law will be limited exclusively to *enforceable* government requests, thus maintaining that they will not voluntarily divulge the private information or their users. In contrast, iCloud's privacy policy appears to be the least respectful of its users' data and is significantly more broad in that it allows access, use, disclosure, or preservation of the data of its users for the purpose of law, national security, legal process, litigation, protection of property rights, fraud prevention or detection, to conform with a government request, or "other issues of public importance." »[507]

Il est évident qu'une attente subjective de vie privée existe lorsque les usagers utilisent des services comme ceux de *Mozy* ou *SpiderOak*. Qu'en est-il cependant lorsque le FSI se réserve le droit d'accéder aux données à sa guise ou à la demande des autorités? Une première piste de solution provient peut-être du fait que la majorité des utilisateurs de services en ligne ne lisent pas les conditions d'utilisation. Certes, une personne qui accepte les conditions d'utilisation est réputée les avoir acceptées, mais il est indéniable que la majorité des consommateurs ne prennent pas le temps de s'enquérir des conditions d'utilisation des services qu'ils utilisent[508].

Plusieurs auteurs soutiennent que l'attente de vie privée demeure valide, même lorsque les conditions de service indiquent que le FSI peut accéder aux données. Cela s'expliquerait notamment par le fait que les conditions de service sont modifiées très fréquemment et unilatéralement par les entreprises, que les lois applicables en matière de protection de la vie privée sont floues et qu'ultimement un utilisateur de services d'infonuagique confie ses données aux FSI pour qu'elles soient sauvegardées et conservées, non pas analysées[509]. Cette conclusion

---

[507] S. K. MIZRAHI, préc., note 447, 316-317, références omises.

[508] Selon une étude effectuée par une professeure à l'Université de New York, moins d'une personne sur 1000 clique sur les liens menant aux conditions de service en ligne (soit environ 0.11%). Voir Andy GREENBERG, « Who Reads The Fine Print Online? Less Than One Person In 1000 », *Forbes*, en ligne : <https://www.forbes.com/sites/firewall/2010/04/08/who-reads-the-fine-print-online-less-than-one-person-in-1000/> (consulté le 15 mai 2018). Par ailleurs, la Cour supérieure et la Cour d'appel ont statué que les conditions d'utilisation imposées par les FSI étaient des contrats d'adhésion, faisant en sorte que les règles du Code civil à leur égard sont applicables. *Mofo Moko c. Ebay Canada Ltd.,* 2013 QCCS 856; *eBay Canada Ltd. c. Mofo Moko*, 2013 QCCA 1912.

[509] A. J. GOLD, préc., note 394, 2341 et 2343; S. J. KOHLS, préc., note 454, 198.

transparaît également de la décision *Spencer*, où une attente raisonnable de vie privée a été reconnue à l'accusé, malgré l'existence de dispositions contractuelles indiquant que le FSI avait le droit de communiquer certaines informations aux policiers[510].

Ultimement, les dispositions contractuelles ou réglementaires sont moins susceptibles d'avoir un impact sur l'attente de vie privée lorsque l'information visée est intrinsèquement intime[511]. Ainsi, bien qu'utiles à l'analyse contextuelle devant être effectuée afin de déterminer si une attente raisonnable de vie privée existe envers les données du *nuage*, ces éléments ne sont pas à eux seuls susceptibles de nier totalement la protection offerte par l'article 8 de la *Charte*.

3.2.3 L'existence d'une attente raisonnable de vie privée sur les données sauvegardées dans le nuage

Concrètement, l'infonuagique n'a fait que déplacer les données personnelles des individus de leur disque dur personnel au serveur d'une entreprise[512]. Est-ce que cette simple migration des données devrait justifier la négation de la protection offerte par l'article 8 de la *Charte* ? Nous ne le pensons pas.

Tel que mentionné au chapitre 1 du présent mémoire, une analyse en quatre étapes est maintenant utilisée par les tribunaux afin de déterminer si une attente raisonnable de vie privée existe. Nous allons donc reprendre ces quatre étapes afin d'en arriver à la conclusion que les données du *nuage* méritent la même protection que les données situées sur l'ordinateur d'un suspect[513].

3.2.3.1 L'objet de la fouille

Les données qu'un individu désire sauvegarder sur le *nuage* peuvent être très variées. Il peut s'agir de données bancaires, de photos personnelles, de documents numérisés, de textes

---

[510] *R.* c. *Spencer*, préc., note 94, par. 56 et suivants.
[511] S. PENNEY, préc., note 263, par. 35.
[512] L. BUCHAN SERAFINO, préc., note 419, 174; S. J. KOHLS, préc., note 454, 198.
[513] *R.* c. *Morelli*, préc., note 11, par. 2.

personnels, de conversations électroniques, de courriels, etc. Tout comme dans les décisions *Morelli*, *Vu* et *Cole*, l'objet de la fouille n'est ici pas le serveur en lui-même, mais bien les données qu'il contient[514].

Selon l'auteur américain David S. Barnhill, une distinction devrait être faite entre les données personnelles qu'un individu a sauvegardées sur son *nuage* et celles que le FSI a créées lors de la sauvegarde des données, c'est-à-dire les métadonnées. Alors que les premières seraient protégées par une attente raisonnable de vie privée, les secondes ne le seraient pas[515]. L'objet de la fouille ne serait donc pas le même dans ces deux situations, ce qui justifierait un traitement différent ultimement en vertu de la *Charte*. Toutefois, certains auteurs prétendent le contraire et soutiennent que les données sauvegardées dans le *nuage* et les métadonnées devraient être protégées, puisque les métadonnées sont également susceptibles de révéler des détails intimes sur les individus[516]. En appliquant les enseignements de la Cour suprême dans l'arrêt *Spencer*, nous pensons, à l'instar de ces auteurs, que les métadonnées devraient être protégées, puisqu'elles ne servent pas seulement à identifier un individu, mais bien à identifier celui-ci par rapport à une utilisation particulière d'Internet[517]. Certes l'attente raisonnable de vie privée est peut-être moindre qu'envers les données personnelles elles-mêmes, mais il n'en demeure pas moins que l'attente existe et est raisonnable.

3.2.3.2 Le droit du demandeur à l'égard de l'objet

Malgré les divergences importantes recensées dans les conditions de service et les politiques concernant la vie privée, tous les FSI indiquent que les données demeurent la propriété du

---

[514] *R.* v. *Craig*, préc., note 484, par. 136 citant; *R.* c. *Morelli*, préc., note 11, par. 2; *R.* c. *Cole*, préc., note 93; *R.* c. *Vu*, préc., note 141.
[515] D. S. BARNHILL, préc., note 421, 645-646; Voir également O. S. KERR, préc., note 284.
[516] Michael W. PRICE, « Rethinking Privacy: Fourth Amendment "Papers" and the Third-Party Doctrine », (2016) 8 *J. Natl. Secur. Law Policy* 247, 250 et 285; Andrew GRAY, « Cloud Atlas - A Map to Amending Metadata Privacy Law in the Modern Era », (2016) 52 *Gonzaga Law Rev.* 147.
[517] *R.* c. *Spencer*, préc., note 94, par. 32.

client[518]. Ainsi, bien que les données soient sauvegardées sur des serveurs appartenant à un tiers, la propriété des données n'est pas transférée à celui-ci.

La propriété de l'appareil électronique utilisé pour accéder aux données n'est pas un élément pertinent à considérer puisque les données du *nuage* peuvent être accédées à partir de n'importe quel appareil avec une connexion Internet. Cette particularité du *nuage* avait d'ailleurs été soulignée dans la décision *Cole*, où la juge Abella, dans sa dissidence, avait indiqué que :

> « comme plus de données sont stockées dans le nuage et qu'on y a accès tant sur l'ordinateur de travail que l'ordinateur personnel, la propriété de l'appareil ou des données, loin de constituer un critère déterminant de l'attente raisonnable en matière de protection de la vie privée, devient un repère de plus en plus inutile »[519].

Lorsqu'il est question de données, le droit du demandeur à l'égard de celles-ci relève principalement du caractère privé des renseignements personnels qu'elles contiennent[520]. En l'espèce, il est indéniable que les données se trouvant dans le *nuage* peuvent « révéler des détails intimes sur le mode de vie et les choix personnels des individus »[521]. Par ailleurs, le droit à la vie privée inclut l'attente que les renseignements que nous divulguons de manière volontaire soient confidentiels et qu'ils ne soient utilisés dans « pour les fins pour lesquelles ils ont été divulgués »[522]. S'ils sont utilisés dans un autre but, « la personne à laquelle se rapportent ces renseignements peut encore conserver une attente raisonnable en matière de protection de la vie privée à leur égard »[523].

Autrement dit, les caractéristiques intrinsèques de l'infonuagique, soit le fait que les données peuvent être accédées à partir de n'importe quel appareil et qu'elles se trouvent sur des serveurs distants, ne doivent pas être utilisées afin de nier le droit du demandeur à l'égard de l'objet. Ainsi, « less emphasis is placed on factors which are of diminished relevance regarding digital

---

[518] D. G. MCCORRY, préc., note 450, 143.
[519] *R.* c. *Cole*, préc., note 94, par. 109.
[520] *R.* c. *Spencer*, préc., note 94, par. 37.
[521] *R.* c. *Plant*, préc., note 99, 293.
[522] *R.* c. *Dyment*, préc., note 27, 430.
[523] *R.* c. *Mills*, [1999] 3 R.C.S. 668, par. 108.

privacy: the medium on which the data is stored and the physical location where storage takes place »[524].

3.2.3.3 L'existence d'une attente subjective

Tel que mentionné au chapitre 1 du présent mémoire, le contexte normatif peut être utilisé afin de déterminer si une attente raisonnable de vie privée existe envers un certain type d'information. Dans le cas des données sauvegardées dans le *nuage*, nous pensons que ce contexte normatif milite pour la reconnaissance d'une attente raisonnable de vie privée. En effet, il existe une supposition sociale selon laquelle nos comptes en ligne font l'objet d'une certaine confidentialité ou d'une certaine vie privée[525]. En ce sens : « a cloud user has placed his files and media into the hands of the third-party cloud provider, and entrusts the third party will store and provide access to the files, but does not expect the provider to look at them. »[526]

Par ailleurs, l'interface utilisée afin d'accéder aux données situées sur le *nuage* ne permet pas toujours de savoir réellement où celles-ci se trouvent. En effet, les fichiers situés dans le *nuage* peuvent parfois être accédés de la même manière que les fichiers se trouvant directement sur le disque dur d'un individu[527]. Dans ces cas, cette interface pourrait donc renforcer l'attente subjective d'un individu selon laquelle ses données sont protégées par la *Charte*. Le fait que les données du *nuage* soient habituellement protégées par mot de passe est également un indice qu'une attente subjective de vie privée est présente[528]. Il importe également de rappeler que l'existence d'une attente subjective de vie privée ne doit pas être un élément difficile à prouver pour un individu réclamant la protection offerte par l'article 9 de la *Charte*[529].

---

[524] D. M. SCANLAN, préc., note 459, 314.
[525] A. J. GOLD, préc., note 394, 2332 et 2337; *R.* v. *Craig*, préc., note 484, par. 121.
[526] S. J. KOHLS, préc., note 454, 198.
[527] M. NIED, préc., note 417, 706; Q. HOCHHALTER, préc., note 451, 178; A. J. GOLD, préc., note 394, 2323; Par exemple, Google Drive peut être installé directement dans un Mac, faisant en sorte que les données sont accessibles de la même manière que celles qui se trouvent uniquement sur le disque dur de l'utilisateur. Voir Tom NELSON, « Setup and Price Guide to Google Drive for the Mac », *Lifewire*, en ligne : <https://www.lifewire.com/how-to-set-up-and-use-google-drive-on-mac-2260845> (consulté le 17 mai 2018).
[528] O. S. KERR, préc., note 285, 1021.
[529] P. BÉLIVEAU et M. VAUCLAIR, préc., note 41, par. 860.

3.2.3.4 Le caractère raisonnable de cette attente subjective, eu égard à l'ensemble des circonstances

Récemment, dans la décision *R.* v. *Craig*, la Cour d'appel de la Colombie-Britannique s'est penchée sur l'attente raisonnable de vie privée que prétendait avoir un accusé envers des données situées sur les serveurs d'une entreprise, donc des données situées dans le *nuage*[530]. Il s'agissait en l'espèce de conversations sur la plateforme *Nexopia*, un réseau social utilisé principalement par des adolescents[531]. La Cour, reprenant les enseignements de la Cour suprême dans la décision *Cole* selon lesquels il n'y a pas de liste de facteurs définitifs permettant d'analyser le caractère raisonnable d'une attente subjective de vie privée[532], a retenu quatre critères principaux afin d'en arriver à la conclusion que l'attente subjective de l'accusé était objectivement raisonnable dans les circonstances.

Premièrement, concernant l'endroit de la fouille, la Cour a conclu que cet élément à lui seul n'appuyait pas l'existence d'une attente raisonnable de vie privée, puisque les données étaient situées sur les serveurs d'un tiers[533]. Toutefois, la Cour a souligné d'un même trait que, de nos jours, une importante partie de nos données ne se trouvent pas sur nos ordinateurs personnels, mais plutôt sur des serveurs. En ce sens, ce n'est pas l'endroit de la fouille qui justifie l'attente de vie privée[534], mais plutôt le contenu des serveurs qui a été créé par l'accusé lui-même[535]. Deuxièmement, la Cour a observé que les messages n'étaient pas à la vue du public, étant protégés par un nom d'utilisateur et un mot de passe, ce qui suggère qu'il y a attente de vie privée[536]. Troisièmement, bien que les messages aient été partagés avec une tierce partie, cela ne rend pas l'attente de vie privée de l'accusé déraisonnable, et ce, pour quatre raisons : le rejet de l'analyse fondée sur le risque dans *Duarte*, l'existence de normes sociales militant pour la reconnaissance d'une attente raisonnable de vie privée dans des messages privés, l'émergence

---

[530] *R.* v. *Craig*, préc., note 484.
[531] *Id.*, par. 3.
[532] *R.* c. *Cole*, préc., note 94, par. 45.
[533] *R.* v. *Craig*, préc., note 484, 101.
[534] « The physical location of data has become an increasingly illogical basis for determining the protection to be afforded data from unreasonable search. » D. M. SCANLAN, préc., note 459, 313.
[535] *R.* v. *Craig*, préc., note 484, par. 103.
[536] *Id.*, par. 104.

de lois prouvant l'existence d'une attente raisonnable de vie privée envers des données partagées avec des tiers et l'émergence d'une jurisprudence au même effet[537]. Quatrièmement, la Cour a souligné que le contenu des messages envoyés par l'accusé soutient le caractère raisonnable de son attente subjective de vie privée, puisqu'ils contiennent des « intimates details of his lifestyle, personal choices, and private identifying information »[538]. Pour ces motifs, la Cour est arrivée à la conclusion que la protection de l'article 8 de la *Charte* est bel et bien applicable aux données de l'accusé qui se trouvaient sur le serveur de l'entreprise *Nexopia*.

Tel que mentionné au chapitre 1, dans la décision *Marakah* la majorité de la Cour suprême a retenu trois critères afin de déterminer si l'attente subjective de l'accusé était raisonnable dans les circonstances : le lieu fouillé, le caractère privé de l'objet de la fouille et le contrôle de l'accusé sur l'objet de la fouille[539]. L'honorable juge McLachlin a alors mentionné qu'une « conversation électronique ne se déroule pas dans un lieu physique précis »[540], ce qui est également pour les données situées dans le *nuage*. Cette constatation n'a toutefois pas empêché la reconnaissance du caractère raisonnable de l'attente de l'accusé dans les circonstances, principalement puisque la protection de l'article 8 de la *Charte* vise les personnes et non les lieux[541]. La majorité a également souligné que « l'absence de contrôle ne porte pas un coup fatal à la reconnaissance d'un intérêt en matière de vie privée »[542], ce qui appuie d'autant plus la conclusion que les données dans le *nuage* sont protégées, malgré leur partage avec le FSI. Par ailleurs, comme la Cour suprême a adopté un principe de neutralité technologique dans son application de l'article 8 de la *Charte*[543], il semble clair que les données personnelles des individus devraient recevoir la même protection et être accédées en vertu des mêmes standards de preuve, peu importe leur emplacement physique[544].

---

[537] *Id.*, par. 105-131.
[538] *Id.*, par. 132.
[539] *R.* c. *Marakah*, préc., note 81, par. 24.
[540] *Id.*, par. 28.
[541] *Hunter* c. *Southam inc.*, préc., note 4, 159.
[542] *R.* c. *Marakah*, préc., note 81, par. 38.
[543] Voir chapitre 2 du présent mémoire.
[544] D. M. SCANLAN, préc., note 459.

Pour l'ensemble de ces raisons, il semble clair que les données situées dans le *nuage* pourront généralement faire l'objet d'une attente raisonnable de vie privée et ainsi bénéficier de la protection prévue à l'article 8 de la *Charte*.

Section 3.3 Les autorisations judiciaires applicables à la saisie des données du *nuage*

Plusieurs scénarios sont susceptibles de se présenter lorsque les policiers voudront accéder à des données situées sur le *nuage* d'un individu sous enquête. En effet, tel que mentionné, dans certains cas, les données seront accessibles directement sur l'ordinateur de l'individu, en raison d'une interface qui permet de consulter les données comme si elles étaient sauvegardées directement sur l'appareil. Ce principe est également applicable aux autres appareils électroniques, qui sont susceptibles d'avoir accès à l'ensemble des données délocalisées d'un individu. Au contraire, certains fournisseurs de services d'infonuagique n'offrent pas cette option et donc les données doivent être accédées par l'entremise d'un site web, à l'aide d'un nom d'utilisateur et d'un mot de passe. De plus, certains fournisseurs peuvent accéder aux données de leurs clients, alors que d'autres ont mis en place une structure sécurisée, ne leur permettant pas de consulter les données.

Nous allons donc poursuivre notre analyse en analysant les diverses autorisations judiciaires susceptibles d'être utilisées afin d'accéder aux données délocalisées se trouvant dans le *nuage*, selon les différents scénarios mentionnés ci-dessus. À ce propos, tel qu'il a été mentionné par un auteur canadien :

> « This dispersion of personal data into the "cloud" can work several different ways. Presuming grounds exist, police may use production orders to obtain data held by commercial entities and thereby not need to meet the higher standard necessary for a warrant to search a person's home. They may seek a warrant for a mobile device and use it to access the suspect's web services and home computer files available to it. They may seek a warrant for a home computer and use it to access any web-based or commercial services it has access to (data on the so-called "cloud"). »[545]

[545] *Id.*, 311.

À cette étape, il est utile de souligner que, comme il y a attente raisonnable de vie privée dans les données du *nuage*, un FSI ne peut consentir à divulguer celles-ci aux forces de l'ordre. Tout comme dans la décision *Cole*, dans laquelle la Cour suprême a décidé qu'un employeur ne pouvait consentir à la saisie à la place de son employé titulaire de l'attente raisonnable de vie privée[546], un FSI ne peut consentir à la remise des données plutôt que le propriétaire des données. Le FSI n'a pas contrôle direct sur les données et n'est pas le propriétaire conjoint de celles-ci avec l'utilisateur des services d'infonuagique[547].

3.3.1 Le mandat de perquisition

Selon l'alinéa 487(2.1)a) C.cr., lorsqu'un mandat de perquisition est exécuté, toutes données auxquelles l'ordinateur (ou un autre appareil électronique) donne accès peuvent être vérifiées. Cette disposition a été interprétée comme autorisant la fouille de données délocalisées, se trouvant sur d'autres ordinateurs accessibles par l'entremise d'un réseau[548]. Cette interprétation semble confirmer que le mandat de perquisition de l'article 487 C.cr. peut être utilisé afin d'accéder à des données situées dans le *nuage*, dans la mesure où ces données sont accessibles à partir de l'ordinateur visé par le mandat de perquisition[549].

Toutefois, cette disposition a été adoptée alors que l'infonuagique n'était qu'à ses balbutiements. En effet, le paragraphe 487(2.1) C.cr. a été ajouté au *Code criminel* en 1997[550], soit bien avant que l'infonuagique ne soit réellement utilisée à grande ampleur. Est-ce donc raisonnable de penser que le législateur canadien avait réellement anticipé qu'autant d'information serait accessible à partir d'un seul ordinateur? Probablement pas. Il est plus plausible que la situation anticipée à l'époque était celle des ordinateurs branchés en réseau local, comme dans une entreprise où les ordinateurs sont tous connectés ensemble. L'auteure

---

[546] *R.* c. *Cole*, préc., note 94, par. 77.
[547] S. J. KOHLS, préc., note 454, 203.
[548] D. M. SCANLAN, préc., note 459, 303; *R. v. Edwards*, [1999] O.J. No. 3819, par. 89.
[549] Dans la décision *R.* v. *Young*, 2012 ONCJ 716, par. 18-19, la Cour mentionne que des données de l'accusé, en l'espèce des images de pornographie juvénile se trouvant dans le nuage, ont été accédées à l'aide d'un mandat de perquisition.
[550] *Code criminel*, L.R.C. 1985, c. 18 (1997), art. 41.

Susan Magotiaux a noté les risques découlant de cette interprétation du paragraphe 487(2.1) C.cr. :

> « The search provisions in the Criminal Code have been updated to address the lack of tangibility and physical presence of digital data. In 1997, section 487 was amended to include provisions aimed directly at the problem of gathering digital "things". Section 487(2.1) and (2.2) provide that, in a regular search warrant under section 487, a police officer or a person at the search location may "use or cause to be used any computer system at the building or place to search any data contained in or available to the computer system". The scope of the subsection has not been widely considered. It is potentially boundless. If taking and examining the desktop box was deemed in R. v. Morelli to be the most intrusive, extensive, and invasive search imaginable, what about a search of all that is "accessible to" that box while its stands connected in a home or office? Depending on the configurations and active connections of a given device, there could be data accessible to the device from other people, other networks, other countries, or other businesses. The section 487 warrant looks for things in a place, yet the Court in Vu recognized that "a search of a computer connected to the Internet or a network gives access to information and documents that are not in any meaningful sense at the location for which the search is authorized". »[551]

Comment donc réconcilier cette disposition avec les développements jurisprudentiels subséquents en matière de nouvelles technologies? L'approche adoptée dans l'arrêt *Vu* serait probablement la meilleure option. Dans cette décision, la Cour suprême a décidé que les ordinateurs ne pouvaient être considérés comme de simples contenants, en raison des intérêts particuliers en matière de vie privée que leur utilisation implique[552]. Ceci a pour conséquence que les policiers doivent spécifiquement indiquer dans leur demande d'autorisation les motifs justifiant la fouille des appareils électroniques se trouvant sur les lieux d'une perquisition, à défaut de quoi ceux-ci ne pourront qu'être saisis – sans être fouillés – avant qu'un second mandat visant spécifiquement leur fouille ne soit obtenu[553].

---

[551] Susan MAGOTIAUX, « Out of Sync: Section 8 and Technologial Advancement in Supreme Court Jurisprudence », (2015) 71 *Supreme Court Law Rev.* 501, par. 26.
[552] *R.* c. *Vu*, préc., note 142, par. 2.
[553] *Id.*, par. 3.

De la même manière, nous pensons que les policiers devraient indiquer dans leur demande d'autorisation les motifs pour lesquels ils désirent accéder au *nuage* d'un individu[554]. Si l'existence d'un *nuage* n'est découverte que lors de la fouille d'un appareil électronique validement saisi, les policiers devraient alors arrêter leurs recherches et obtenir un nouveau mandat avant d'accéder au *nuage*. Le juge émetteur serait alors en mesure d'évaluer les diverses implications en matière de vie privée et, dans certains cas, imposer des protocoles de saisie, notamment lorsque les données du *nuage* sont également accessibles par des tiers innocents.

Par ailleurs, nous pensons que l'application de la doctrine des objets bien en vus ne pourrait ici permettre la fouille du *nuage* sans l'obtention d'une autorisation judiciaire séparée. Puisque le *nuage* peut être considéré comme un lieu distinct en matière de fouille, autant physiquement que virtuellement[555], la première condition pour que la théorie s'applique, soit que « the seizing officer must be lawfully in the place of seizure »[556], ne serait pas remplie.

Tel qu'il a été mentionné au chapitre 1, les policiers peuvent parfois contourner l'exigence de l'obtention préalable d'un mandat en raison de l'urgence de la situation. Certains pourraient prétendre que le risque de destruction des données dans le *nuage* constitue une situation urgente justifiant l'application de cette doctrine d'exception, puisque les données peuvent être détruites à partir d'un autre appareil ayant une connexion Internet. Or, le risque de perte des données est moins important que ce qui pourrait sembler. En effet,

> « even after a user deletes his data or closes his account, many cloud storage providers will preserve data on their servers for a period of time. […] Simply deleting data from a drive does not completely destroy the files hosted there, and "deleted" data is actually recoverable. »[557]

---

[554] Certains auteurs suggèrent qu'un mandat séparé soit obtenu, voir S. J. KOHLS, préc., note 454, 201. Dans la mesure où les policiers indiquent spécifiquement dans leur demande d'autorisation les motifs expliquant la fouille du nuage, nous ne pensons pas que cette exigence soit nécessaire.
[555] A. J. GOLD, préc., note 394, 2345.
[556] *R.* v. *Atkinson*, préc., note 178, par. 57.
[557] A. J. GOLD, préc., note 394, 2347.

Par ailleurs, l'existence de l'ordre et de l'ordonnance de préservation de données sont également accessibles aux policiers s'ils jugent qu'il y a un risque de destruction.

Somme toute, nous pensons que le paragraphe 487(2.1) C.cr. peut permettre la saisie des données situées dans le *nuage*, dans la mesure où le mandat de perquisition émis spécifie que cela est permis. Cela veut dire que dès qu'un appareil électronique d'un suspect est validement saisi, l'entièreté de ses données délocalisées pourront être accédées et analysées par les forces de l'ordre. Cette autorisation judiciaire sera donc la plus pertinente dans le scénario où les données sont accessibles directement à partir de l'appareil électronique de l'individu ou lorsque les policiers ont accès aux mots de passe utilisés par le suspect afin de se connecter à ses services d'infonuagique par le biais d'Internet. Si cela n'est pas le cas, l'ordonnance générale de communication sera probablement plus appropriée.

3.3.2 L'ordonnance générale de communication

Contrairement aux objets qui sont normalement visés par un mandat de perquisition ou aux données se trouvant dans l'ordinateur d'un suspect, les données du *nuage* sont très souvent accessibles par une tierce personne, soit le FSI. Cet accès supplémentaire simultané[558], qui n'existe pas habituellement en matière de fouille, peut devenir un avantage intéressant pour les policiers qui pourront alors accéder aux données par l'entremise du FSI, sans que le suspect ne soit mis au courant immédiatement. Cela aurait également comme avantage de pouvoir contourner un mot de passe qui bloquerait l'accès aux données à partir de l'ordinateur de l'accusé, sous réserve des particularités discutées à la section 2.3.1 du présent mémoire.

Dans le cas des données personnelles sauvegardées par l'individu sur un *nuage*, l'ordonnance générale de communication pourra être utilisée par les policiers afin de contraindre un FSI à divulguer celles-ci. Considérant que cette ordonnance peut être obtenue en respectant le même standard d'émission qu'un mandat de perquisition, soit l'existence de *motifs raisonnables de croire*, il semble que l'utilisation de cette technique d'enquête soit raisonnable, compte tenu du

[558] D. M. SCANLAN, préc., note 459, 312.

degré d'attente de vie privée élevé applicable à ces données[559]. Dans ce cas, le FSI deviendrait alors un agent de l'État en exécutant saisissant les données visées par l'ordonnance de communication[560].

Certains auteurs critiquent toutefois l'utilisation de telles ordonnances afin d'accéder aux données situées sur le *nuage*. Selon Christopher Soghoian, afin que la vie privée des usagers du *nuage* soit respectée, les données devraient être cryptées *de facto*, afin que les FSI ne puissent y avoir accès[561], ce que les entreprises *SpiderOak* et *Mozy* font déjà. Selon lui, cette mesure aurait pour effet de rétablir l'équilibre entre le droit des individus au respect de leur vie privée et l'intérêt légitime de l'État à réprimer le crime. L'État pourrait alors utiliser d'autres méthodes d'enquête, en utilisant le mandat général de l'article 487.01 C.cr., afin d'accéder aux données non cryptées ou pour obtenir les mots de passe et clés de cryptage utilisés par le suspect[562].

A contratrio, d'autres auteurs soulignent que le cryptage et les autres mesures de protection des données pourraient empêcher totalement les forces de l'ordre d'avoir accès aux données, ce qui ne serait pas souhaitable[563]. Dans certains cas, si les données du *nuage* sont protégées par mot de passe ou par cryptage, il sera en effet possible que les données soient complètement inaccessibles, malgré l'utilisation de logiciels tentant de déchiffrer les clés de cryptage utilisées. Cette situation s'est notamment présentée dans la décision *Pratchett*, dans laquelle un système d'infonuagique personnel (ou un *nuage privé*), constitué de quatre disques durs saisis sur les lieux de la perquisition, n'a pu être accédé en raison de la complexité du système de cryptage en place[564].

---

[559] Voir section 1.1.3 du présent mémoire.
[560] J. DYKSTRA et D. RIEHL, préc., note 415, 35.
[561] Christopher SOGHOIAN, « Caught in the Cloud: Privacy, Encryptions, and Government Back Doors in the Web 2.0 Era », (2010) 8 *J. Telecommun. High Technol. Law* 359, 398. Voir également W. C. LIN, préc., note 476.
[562] L'auteur mentionne notamment l'utilisation de la technique « black bag job », qui inclut des entrées subreptices ou l'utilisation de surveillance électronique. C. SOGHOIAN, préc., note 561, 398. Voir également la section 2.3.2 du présent mémoire à ce sujet.
[563] S. W. BRENNER, préc., note 354, 534.
[564] *R.* v. *Pratchett*, 2016 SKPC 19, par. 74-78.

3.3.3 Le mandat général

Par ailleurs, qu'arrive-t-il si le FSI décide de ne pas collaborer et de ne pas respecter l'ordonnance de communication? Les policiers se trouveraient alors devant deux choix : saisir les serveurs du FSI, ce qui inclut l'accès à toutes les données s'y trouvant, y compris celles appartenant à des tiers innocents, ou encore d'utiliser des techniques d'accès à distance au *nuage*[565]. La première option semble à première vue laborieuse en raison de la quantité impressionnante de données que peuvent contenir de tels serveurs, mais elle n'est pas impossible même si les données sont situées à l'étranger tel que démontré par un renvoi de la Cour supérieure de l'Ontario où la *Loi sur l'entraide juridique en matière criminelle*[566] a été appliquée afin de saisir le contenu de serveurs se trouvant au Canada, dans le cadre d'une enquête menée par les Pays-Bas[567]. Concernant la seconde option, un tel accès à distance devrait selon toute vraisemblance être autorisé par l'entremise d'un mandat général de l'article 487.01 C.cr., puisqu'il s'agit d'une technique d'enquête inusitée équivalent à une entrée subreptice[568].

Il est maintenant connu que les autorités ont la capacité technologique d'intercepter les données alors qu'elles sont en transit vers le *nuage*[569]. Cette technique a toutefois été vivement critiquée aux États-Unis puisqu'elle a été utilisée dans le cadre d'une opération de surveillance de masse par la *National Security Agency* (NSA), ce qui avait été révélé par le lanceur d'alerte Edward Snowden[570]. Cette technique devrait également être autorisée par mandat général au Canada, s'il s'avère que les autorités canadiennes ont également cette capacité technologique.

---

[565] S. K. MIZRAHI, préc., note 447, 321.
[566] *Loi sur l'entraide juridique en matière criminelle*, L.R.C. 1985, c. 30.
[567] *Mutual Legal Assistance in Criminal Matters Act (Re)*, 2016 ONSC 5699, par. 10-11. Dans la decision, la Cour adresse également la problématique de l'accès aux données de tiers.
[568] Susan W. BRENNER, « Law, Dissonance, and Remote Computer Searches », (2012) 24 *N. C. Journal Law Technol.* 43, 61.
[569] Joris V. J. VAN HOBOKEN, « Privacy and Security in the Cloud: Some Realism about Technical Solutions to Transnational Surveillance in the Post-Snowden Era », (2014) 66 *Maine Law Rev.* 487.
[570] *Id.*

3.3.4 Les ordonnances de communication spécifiques

À la section 3.2.3.1, nous avons conclu que les métadonnées peuvent également être l'objet d'une attente raisonnable de vie privée. Une autorisation judiciaire est donc également nécessaire à leur saisie. Toutefois, certaines ordonnances de communication spécifiques sont susceptibles de s'appliquer, permettant plus facilement la saisie de ces données en raison du seuil plus bas nécessaire à leur obtention, soit celui des *motifs raisonnables de soupçonner*. Il s'agirait principalement de l'ordonnance de communication en vue de retracer des communications données (487.015 C.cr.) et de l'ordonnance de communication – données de transmission (487.016 C.cr.). Ces ordonnances pourraient par exemple être utilisées afin d'identifier un ordinateur accédant au *nuage*, par l'entremise d'une adresse IP particulière, ou encore afin d'obtenir le registre des connexions au *nuage*, avec la date, l'heure et l'appareil ayant été utilisé afin de se connecter[571].

3.3.5 Conclusion sur les ordonnances judiciaires applicables

Somme toute, selon la stratégie policière mise de l'avant, les forces de l'ordre sont susceptibles de recourir à diverses autorisations judiciaires, que ce soit séparément ou ensemble. Il se pourrait effectivement que plusieurs autorisations soient nécessaires et pertinentes, par exemple dans le cas où certaines données sont protégées par mot de passe et d'autres non. Malgré tout cela, une constante demeure pour les autorités : l'obligation d'obtenir une autorisation judiciaire préalable, en raison de l'existence d'une attente raisonnable de vie privée visant les données du *nuage* et les métadonnées y étant rattachées.

Devant la multiplication des données se trouvant dans le *nuage*, il est clair que les FSI seront de plus en plus sollicités par l'entremise d'ordonnances de communication diverses. À ce sujet, il est intéressant de noter que l'individu ou l'entreprise qui obtempère à une telle ordonnance ne peut se faire dédommager pour les frais encourus afin de respecter celle-ci[572]. Par ailleurs, l'article 487.0195 C.cr. prévoit qu'aucune autorisation judiciaire n'est requise lorsque la tierce

---

[571] J. DYKSTRA et D. RIEHL, préc., note 415, 22.
[572] *Société Télé-Mobile* c. *Ontario*, [2008] 1 R.C.S. 305.

partie consent à remettre les données, ce qui risque toutefois de ne pas trouver application en matière d'infonuagique en raison de l'intérêt des entreprises à respecter la vie privée de leurs clients.

Section 3.4 La procédure à suivre lors de la saisie de ces données

Outre les considérations technologiques générales applicables aux données informatiques qui ont été survolées à la section 2.2.2, certaines spécificités s'appliquent à la saisie de données dans le *nuage*. D'abord, lorsque l'accès au *nuage* est effectué par le FSI, en vertu d'une ordonnance de communication, il est incertain si celui-ci sera en mesure de fournir aux autorités une copie miroir des données et s'il sera en mesure de récupérer des données supprimées. En effet, « although cloud providers likely know when files in their storage array are deleted and althought they may have logs to prove it, they probably lack the ability to recover deleted files or to produce complete hard disk images »[573].

Ensuite, puisque l'enquêteur attitré à l'analyse des données n'aura généralement pas accès à l'appareil électronique en tant que tel (soit le serveur qui est la propriété du FSI), mais plutôt à une copie des données s'y trouvant, certains éléments ne pourront pas être examinés, comme la mémoire vive[574]. Cette particularité du *nuage* peut également compliquer le travail des enquêteurs qui ne pourront pas toujours copier les données sur un disque dur afin de pouvoir les examiner[575]. Dans ces cas, il est suggéré que les enquêteurs filment ou prennent des photos des données telles qu'elles apparaissent à l'écran alors qu'elles sont consultées. De plus, l'interface du *nuage* apparaissant à l'écran pourrait être différent pour un enquêteur que pour le suspect, lorsque le *nuage* est accédé directement à partir d'un site web[576]. Il se pourrait donc que des différences mineures doivent être expliquées en Cour.

---

[573] J. DYKSTRA et D. RIEHL, préc., note 415, 25.
[574] Terrence LILLARD (dir.), *Digital forensics for network, Internet, and cloud computing: a forensic evidence guide for moving targets and data*, Burlington, MA, Syngress, 2010, p. 11.
[575] *Id.*, p. 282.
[576] *Id.*, p. 283.

L'enquêteur effectuant la saisie des données dans le *nuage* ne pourra employer les mêmes techniques qui sont normalement utilisées lorsque des données sont saisies directement à partir d'un appareil appartenant au suspect, comme un disque dur ou un cellulaire. En effet, si tel était le cas, l'enquêteur obtiendrait toutes les données situées dans le *nuage*, y compris celles des autres clients du FSI ayant des données sur ce serveur spécifique[577].

Par ailleurs, en raison du volume important de données pouvant se trouver dans le *nuage* d'un individu, le coût de collecte et d'analyse de ces données peut être très élevé[578]. Il se pourrait donc que des situations se présentent où le coût anticipé soit trop élevé, par rapport à la force probante de la preuve pouvant être découverte.

Section 3.5 Survol des considérations de juridiction

Une controverse jurisprudentielle et doctrinale existe actuellement sur l'application extraterritoriale des ordonnances de communication prévues au *Code criminel*. En effet, certains croient que les ordonnances de communication peuvent avoir une portée extraterritoriale, tandis que d'autres prétendent que la communication de telles données doit se faire selon les règles applicables du pays où sont situés les serveurs.

La Cour d'appel de la Colombie-Britannique a jugé qu'une ordonnance générale de communication pouvait être utilisée afin d'obtenir la communication de données détenues par une entreprise américaine n'ayant qu'une présence virtuelle au Canada[579]. Ainsi, l'entreprise américaine *Craigslist* a dû remettre des documents aux autorités canadiennes, en vertu d'une ordonnance générale de communication, bien que l'entreprise ait son siège social en Californie et que l'emplacement géographique exact des données recherchées était inconnu[580]. À l'appui de sa décision, la Cour souligne notamment que le résumé législatif du projet de loi C-13 indique que les diverses ordonnances de communication peuvent effectivement être utilisées afin

---

[577] Ann D. ZEIGLER et Ernesto F. ROJAS, *Preserving electronic evidence for trial: a team approach to the litigation hold, data collection, and evidence preservation*, Boston, Elsevier, 2016, p. 112.
[578] Kenneth N. RASHBAUM, Bennett BORDEN et Theresa H. BEAUMONT, « Outrun the Lions: A Practical Framework for Analysis of Legal Issues in the Evolution of Cloud Computing », (2014) 12 *Ave Maria Law Rev.* 71, 97.
[579] *British Columbia (Attorney General)* v. *Brecknell*, 2018 BCCA 5.
[580] *Id.*, par. 14.

d'obtenir des documents se trouvant dans un autre pays[581]. La Cour retient également que la distinction entre présence physique et présence virtuelle est maintenant illusoire :

> « In the second place, in the Internet era it is formalistic and artificial to draw a distinction between physical and virtual presence. Corporate persons, as I have noted, can exist in more than one place at the same time. With respect, I do not think anything turns on whether the corporate person in the jurisdiction has a physical or only a virtual presence. To draw on and rely on such a distinction would defeat the purpose of the legislation and ignore the realities of modern day electronic commerce. Moreover, the current facts illustrate the doubtful relevance of the distinction. Craigslist's virtual presence is closely connected to the circumstances of the alleged offence, because at least some elements of the alleged offence were facilitated by relying on the services Craigslist provides virtually. In terms of the alleged offence, any physical presence Craigslist may have in the jurisdiction is beside the point. A corporate entity's physical presence may have nothing to do with the circumstances of an offence. In my view, it would be curious if the presence of a retail outlet which is totally unrelated to the acquisition of information sought by a production order would ground a jurisdiction that did not otherwise exist. »[582]

Tandis que la Cour d'appel de la Colombie-Britannique a appuyé son raisonnement sur la présence virtuelle du FSI au Canada, une interprétation qui semble être partagée par les auteurs Fontana et Keeshan[583], le paragraphe 487(2.1) C.cr. a également été interprété comme autorisant des saisies à distance, sur des serveurs se trouvant de l'autre côté de la frontière[584].

Parallèlement, la Cour fédérale a conclu que des documents accessibles au Canada, mais qui se trouvent dans un autre pays, peuvent être visés par une demande de communication en vertu de la *Loi de l'impôt sur le revenu*[585]. Selon la Cour :

> « […] On ne peut pas vraiment prétendre que ces renseignements "résident" en seul endroit ou qu'ils "appartiennent" à une seule personne. La réalité est que les renseignements peuvent être obtenus facilement et instantanément par les personnes qui font partie du groupe des entités de eBay dans divers endroits. Il importe peu de savoir où se trouvent les renseignements conservés électroniquement et de savoir quelle entité, le cas échéant, par entente ou autrement, revendique la "propriété" de ces renseignements. Ils se "situe[nt] à la

---

[581] J. NICOL et D. VALIQUET, préc., note 306, p. 13.
[582] *British Columbia (Attorney General)* v. *Brecknell*, préc., note 579, par. 40.
[583] J. A. FONTANA et D. KEESHAN, préc., note 74, p. 494.
[584] S. K. MIZRAHI, préc., note 447, 346.
[585] *Loi de l'impôt sur le revenu*, L.R.C. 1985, c. 1 (5e suppl.).

> fois ici et à l'autre endroit" pour reprendre les mots du juge Binnie au paragraphe 59 de l'arrêt *Société canadienne des auteurs, compositeurs et éditeurs de musique c. Association canadienne des fournisseurs Internet*, [2004] 2 R.C.S. 427. […] »[586]

Cette décision a été confirmée par la Cour d'appel fédérale, qui se demande « [q]ui, après tout, se rend à l'emplacement des serveurs pour lire les renseignements qui y sont stockés? »[587] Les auteurs Halladay et Chad prétendent toutefois que les conclusions de la Cour fédérale et de la Cour d'appel fédérale dans ce dossier ne s'appliquent qu'aux données qui sont utilisées de manière fréquente et usuelle par les employés d'une entreprise, non pas à toutes les données auxquelles ces individus ont accès[588].

De son côté, la Cour provinciale de Terre-Neuve et Labrador a plutôt conclu que l'ordonnance générale de communication ne pouvait être utilisée pour obtenir les données se trouvant physiquement hors du Canada[589]. Bien que jugeant valides les préoccupations soulevées par les juges de la Colombie-Britannique en ce qui concerne les difficultés d'enquêter sur des crimes ayant une portée extraterritoriale, le juge Gorman a conclu que la disposition ne peut avoir une portée extraterritoriale, en appliquant les enseignements de l'arrêt *Hape*[590]. Selon la Cour, le Parlement aurait dû mentionner expressément que la disposition peut avoir une portée extraterritoriale, si tel était son intention[591]. La Cour semble donc conclure que le recours à la *Loi sur l'entraide juridique en matière criminelle* est nécessaire, malgré les problèmes que pose son application[592].

De la même manière, aux États-Unis, un tribunal a conclu que la communication de données situées sur un serveur en Irlande ne pouvait être autorisée en vertu des lois américaines. Bien que le juge émetteur eût autorisé la communication des données situées en Irlande, au motif que

---

[586] *eBay Canada Limited* c. *Canada (Revenu national)*, 2007 CF 930, par. 23.
[587] *eBay Canada Ltd.* c. *M.R.N.*, 2010 RCF 145, par. 48.
[588] Casey W. HALLADAY et Joshua CHAD, « A Database Too Far? Interpreting the Competition Bureau's Computer Search Powers », (2014) 27 *Can. Compet. Law Rev.* 453, 459.
[589] *In the matter of an application to obtain a production order pursuant to section 487.014 of the Criminal Code of Canada*, 2018 NLPC 2369.
[590] *R.* c. *Hape*, [2007] 2 R.C.S. 292.
[591] *In the matter of an application to obtain a production order pursuant to section 487.014 of the Criminal Code of Canada*, préc., note 589, par. 24.
[592] *Loi sur l'entraide juridique en matière criminelle*, préc., note 566.

l'entreprise avait contrôle sur les données à partir des États-Unis, ce qui était suffisant afin d'en autoriser la communication en vertu des lois américaines, et non irlandaises[593], la Cour siégeant en révision a plutôt conclu à l'inverse[594]. Toutefois, une nouvelle loi a depuis été adoptée aux États-Unis, rendant la décision de la Cour siégeant en révision sans objet. En effet, le *Clarifying Lawful Overseas Use of Data Act* (CLOUD Act) prévoit maintenant que les ordonnances judiciaires américaines peuvent être utilisées afin d'obtenir ou de saisir des données situées à l'étranger[595]. Il est intéressant de souligner que plusieurs FSI se sont réjouis de l'adoption de cette loi, tandis que la majorité des groupes de défense des droits des usagers d'Internet se sont plutôt prononcés contre son adoption[596].

Dans tous les cas, ces questions risquent d'être analysées tôt ou tard par la Cour suprême, ou alors par le législateur canadien, considérant leur importance et le fait que la majorité des grands sites web ne sont pas administrés par des entreprises canadiennes. Les notions de présence virtuelle, de contrôle et d'accès risquent donc d'être importantes dans cette analyse.

---

[593] *In re* Warrant to Search a Certain E-mail Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466 (S.D.N.Y. 2014).
[594] *In re* Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corp., 829 F. 3d. 197, 200-01 (2nd Cir. 2016).
[595] *Clarifying Lawful Overseas Use of Data (CLOUD) Act*, H.R. 4943, 115th Cong. (2018).
[596] Aaron MAK, « Congress Put the Controversial CLOUD Act in Its Spending Bill. What Does That Mean For Data Privacy? », *Slate Magazine* (22 mars 2018), en ligne : <https://slate.com/technology/2018/03/cloud-act-microsoft-justice-department-omnibus-spending-bill.html> (consulté le 20 mai 2018); Mary Jo FOLEY, « Microsoft bullish on Congress' inclusion of CLOUD Act in funding bill », *ZDNet*, en ligne : <https://www.zdnet.com/article/microsoft-bullish-on-congress-inclusion-of-cloud-act-in-funding-bill/> (consulté le 20 mai 2018).

Conclusion

À travers les années, la Cour suprême a tenté d'adapter les principes généraux applicables aux fouilles, saisies et perquisitions aux réalités contemporaines soulevées par l'arrivée de nouvelles technologies. Toutefois, il semble que cette adaptation ne soit pas entièrement cohérente à certains égards. Il nous semble en effet contradictoire que la Cour suprême reconnaisse d'emblée que les fouilles d'ordinateur soient envahissantes et attentatoires à la vie privée[597], tandis que les téléphones reçoivent une protection moindre dans le cas d'une arrestation, malgré la quantité importante de données auxquelles ils peuvent donner accès[598]. En ce sens, la dissidence de *Fearon*, signée par la juge Karakatsanis, nous semble cadrer davantage avec les décisions précédentes de la Cour suprême lorsqu'il s'agit « de réaliser une mise en équilibre effective et impartiale des objectifs de l'État en matière d'application de la loi et des intérêts des gens au respect de leur vie privée en ce qui concerne leurs ordinateurs personnels »[599]. Malgré cela, les développements récents en cette matière constituent néanmoins un pas dans la bonne direction lorsqu'il s'agit de reconnaître un droit à la vie privée pour les usagers des nouvelles technologies.

Le rejet de l'approche fondée sur le risque par la Cour suprême dans l'arrêt *Duarte* semble au cœur de cette adaptation des anciens principes découlant de l'application de l'article 8 de la *Charte* aux nouvelles réalités du monde virtuel. En effet, cette décision a récemment retrouvé son importance dans l'arrêt *Marakah*, où la majorité a réitéré le fait que le risque qu'un tiers divulgue notre information à l'État n'est pas un élément suffisant afin de nier la protection constitutionnelle contre les fouilles, perquisitions ou saisies abusives[600]. De plus, comme nous l'avons vu, l'arrêt *Duarte* est également central à la reconnaissance d'une attente raisonnable de vie privée envers les données du *nuage*.

---

[597] *R.* c. *Morelli*, préc., note 11, par. 2.
[598] *R.* c. *Fearon*, préc., note 133.
[599] *Id.*, par. 105, dans la dissidence de la juge Karakatsanis.
[600] *R.* c. *Marakah*, préc., note 81, par. 40.

En analysant les principes généraux applicables aux fouilles, saisies et perquisitions et l'application de ces principes aux fouilles d'appareils électroniques, nous avons effectivement pu conclure que les données délocalisées situées dans le *nuage* méritent également la protection de la *Charte*. À travers l'analyse contextuelle développée par la Cour suprême, il semble clair que l'emplacement des données ainsi que leur partage avec un tiers ne peuvent permettre de nier la reconnaissance d'une attente raisonnable de vie privée aux propriétaires des données.

Malgré cette reconnaissance, la protection réelle de ces données est quelque peu amenuisée par les multiples ordonnances judiciaires pouvant être utilisées afin de procéder à leur saisie. En effet, tandis que les données situées dans un ordinateur ne peuvent être obtenues que par mandat de perquisition, les données situées dans le *nuage* peuvent également être obtenues avec des ordonnances de communication, par l'entremise du FSI. Bien que pouvant être décriée, cette multiplication des ordonnances applicables peut également être perçue comme une manière de rétablir la capacité de l'État d'enquêter et d'obtenir de telles données informatiques ; un procédé qui n'est pas sans heurt. En effet, la saisie des données situées dans le nuage est confrontée à plusieurs complications qui n'existent pas dans le monde réel. Mots de passe, cryptage, serveurs situés dans le monde entier… tous des éléments qui peuvent ralentir le travail des autorités dans des dossiers déjà complexes. La possibilité de recourir à diverses autorisations judiciaires serait alors une manière de rétablir le droit de l'État de lutter contre la criminalité.

De plus, une fois les données saisies et analysées, les problèmes ne sont pas nécessairement terminés. L'admissibilité en preuve des données du *nuage* n'est pas bien définie à l'heure actuelle[601]. D'abord, l'authenticité de ces données peut être difficile à établir, puisque plusieurs personnes peuvent y accéder, souvent en simultané. De plus, le *nuage* est un environnement numérique complexe dont l'analyse ne fait pas consensus à travers les différents spécialistes[602].

---

[601] Voir notamment K. N. RASHBAUM, B. BORDEN et T. H. BEAUMONT, préc., note 578, 98 et suivantes.
[602] J. DYKSTRA et D. RIEHL, préc., note 415, 38 et 43.

Pour cette raison et puisqu'il s'agit d'une technologie qui est en constante évolution, la fiabilité du *nuage* peut être sujette à discussion devant les tribunaux[603].

Dans quelques années, lorsque la problématique relative à la saisie des données du *nuage* sera bel et bien réglée, le droit criminel canadien se retrouvera vraisemblablement devant une autre technologie susceptible de soulever les débats et les discussions animés. Selon l'état actuel des technologies les plus répandues, il est plausible que cette problématique soit celle de l'Internet des objets (ou *Internet of things*)[604]. Cette notion désigne une multitude d'objets qui peuvent être dotés d'une connexion Internet : « Internet-connected televisions, light switches, washing machines, electrical meters, Barbie dolls, self-driving cars, and even toilets »[605]. Ces objets connectés sont susceptibles de révéler des détails intimes sur le mode de vie de leurs propriétaires, non seulement à la manière de données informatiques, mais plutôt comme le ferait un dossier médical. Il sera donc particulièrement important pour les tribunaux de rester à l'affût de ces technologies dans les prochaines années, afin que le droit criminel ne se trouve pas en décalage par rapport à la réalité technologique applicable.

---

[603] Au sujet de la fiabilité des sciences nouvelles, voir *R.* c. *J.-L.J.*, [2000] 2 R.C.S. 600; *R.* c. *Trochym*, [2007] 1 R.C.S. 239.
[604] La traduction de cette notion est issue de WIKIPEDIA, « Internet des objets », dans Wikipédia, en ligne : <https://fr.wikipedia.org/w/index.php?title=Internet_des_objets&oldid=147938653> (consulté le 22 mai 2018).
[605] N. RICHARDS, préc., note 480, 1483.

TABLE DE LA LÉGISLATION

Textes constitutionnels

Charte canadienne des droits et libertés, partie I de la *Loi constitutionnelle de 1982*, [annexe B de la *Loi de 1982 sur le Canada*, 1982, c. 11 (R.-U.)], [ci-après la Charte].

Textes fédéraux

Code criminel, L.R.C. 1985, c. C-46.

Loi concernant la déclaration obligatoire de la pornographie juvénile sur Internet par les personnes qui fournissent des services Internet, L.C. 2011, c. 4.

Loi de l'impôt sur le revenu, L.R.C. 1985, c. 1 (5e suppl.).

Loi modifiant le Code criminel, la Loi sur la preuve au Canada, la Loi sur la concurrence et la Loi sur l'entraide juridique en matière criminelle, projet de loi n°C-13 (sanctionné – 9 décembre 2014), 2e sess., 41e légis. (Can.).

Loi sur la preuve au Canada, L.R.C. 1985, c. C-5.

Loi sur la protection des renseignements personnels et les documents électroniques, L.C. 2000, c. 5.

Loi sur l'entraide juridique en matière criminelle, L.R.C. 1985, c. 30.

Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes, L.C. 2000, c. 17.

Loi sur les banques, L.C. 1991, c. 46.

Loi sur les douanes, L.R.C. 1985, c. 1 (2e suppl.).

Textes québécois

Charte des droits et libertés de la personne, L.R.Q., c. C-12.

Textes étrangers et internationaux

Clarifying Lawful Overseas Use of Data (CLOUD) Act, H.R. 4943, 115th Cong. (2018).

Convention sur la cybercriminalité, 23 novembre 2001, S.T.E. nº 185 (entrée en vigueur au Canada le 1er novembre 2015).

Victims of Child Abuse Act, (1990), U.S. Code, Title 18 – Crimes and Criminal Procedure, Chapter 110.

TABLE DES JUGEMENTS

Jurisprudence canadienne

Ontario (Ministry of the Attorney General) v. *Law Society of Upper Canada*, 2010 ONSC 2150.

Québec (Procureur général) c. *Laroche*, [2002] 3 R.C.S. 708.

R. c. *2952-1366 Québec inc.*, 2000 CanLII 10009 (QC CA).

R. c. *A.M.*, [2008] 1 R.C.S. 569.

R. c. *Araujo*, [2000] 2 R.C.S. 992.

R. c. *Arp*, [1998] 3 R.C.S. 339.

R. c. *Beare*, [1988] 2 R.C.S. 387.

R. c. *Big M Drug Mart*, [1985] 1 R.C.S. 295.

R. c. *Boudreau-Fontaine*, 2010 QCCA. 1108.

R. c. *Borden*, [1994] 3 R.C.S. 145.

R. c. *Bottineau*, 2011 ONCA 194.

R. c. *Buhay*, [2003] 1 R.C.S. 631.

R. c. *Caslake*, [1998] 1 R.C.S. 51.

R. c. *Colarusso*, [1994] 1 R.C.S. 20.

R. c. *Cole*, [2012] 3 R.C.S. 34.

R. c. *Collins*, [1987] 1 R.C.S. 265.

R. c. *Cornell*, [2010] 2 R.C.S. 142.

R. c. *Debot*, [1989] 2 R.C.S. 1140.

R. c. *Desjardins*, 2014 QCCS 6695.

R. c. *Duarte*, [1990] 1 R.C.S. 30.

R. c. *Dyment*, [1988] R.C.S. 417.

R. c. *Edwards*, [1996] 1 R.C.S. 128.

R. c. *Evans*, [1996] 1 R.C.S. 8.

R. c. *Fearon*, [2014] 3 R.C.S. 621.

R. c. *Feeney*, [1997] 2 R.C.S. 13.

R. c. *Golden*, [2001] 3 R.C.S. 679.

R. c. *Gomboc*, [2010] 3 R.C.S. 211.

R. c. *Grant*, [1993] 3 R.C.S. 223.

R. c. *Grant*, [2009] 2 R.C.S. 353.

R. c. *Guérin*, 2011 QCCQ 57.

R. c. *Hape*, [2007] 2 R.C.S. 292.

R. c. *Harrison*, [2009] 2 R.C.S. 494.

R. c. *H.-G.*, 2005 QCCA 1160.

R. c. *Jones*, [2017] 2 R.C.S. 696.

R. c. *J.-L.J.*, [2000] 2 R.C.S. 600.

R. c. *Kokesh*, [1990] 3 R.C.S. 3.

R. c. *Law*, [2002] 1 R.C.S. 227.

R. c. *Lenneville*, 2007 QCCA 400.

R. c. *MacDonald*, [2014] 1 R.C.S. 37.

R. c. *Maheux*, 2016 QCCQ 19690.

R. c. *Mann*, [2004] 3 R.C.S. 59.

R. c. *Marakah*, [2017] 2 R.C.S. 608.

R. c. *Mellenthin*, [1992] 3 R.C.S. 615.

R. c. *Mills*, [1999] 3 R.C.S. 668.

R. c. *Morelli*, [2010] 1 R.C.S. 253.

R. c. *Nolet*, [2010] 1 R.C.S. 851.

R. c. *Paterson*, [2017] 1 R.C.S. 202.

R. c. *Patrick*, [2009] 1 R.C.S. 579.

R. c. *Plant*, [1993] 3 R.C.S. 281.

R. c. *Rodgers*, [2006] 1 R.C.S. 554.

R. c. *Silveira*, [1995] 2 R.C.S. 297.

R. c. *Shin*, 2012 ONCA 707.

R. c. *Société TELUS Communications*, [2013] 2 R.C.S. 3.

R. c. *Spencer*, [2014] 2 R.C.S. 212.

R. c. *Stevenson George Alles*, 2014 QCCQ 12000.

R. c. *Stillman*, [1997] 1 R.C.S. 607.

R. c. *Strachan*, [1988] 2 R.C.S. 980.

R. c. *Suberu*, [2009] 2 R.C.S. 460.

R. c. *Tessling*, [2004] 3 R.C.S. 341.

R. c. *Thompson*, [1990] 2 R.C.S. 1111.

R. c. *Tremblay*, 2001 QCCQ 24412.

R. c. *Trochym,* [2007] 1 R.C.S. 239.

R. c. *Trudeau*, 2016 QCCQ 925.

R. c. *Tse*, [2012] 1 R.C.S. 531.

R. c. *White*, [1999] 2 R.C.S. 417.

R. c. *Wise*, [1992] 1 R.C.S. 527.

R. c. *Wong*, [1990] 3 R.C.S. 36.

R. c. *Vu*, [2013] 3 R.C.S. 657.

Renvoi sur l'écoute électronique, [1984] 2 R.C.S. 697.

Re Subscriber Information, 2015 ABPC 178.

R. v. *Atkinson*, 2012 ONCA 380.

R. v. *Bishop*, 2007 ONCJ 441.

R. v. *Branton*, 2001 CanLII 8535 (ON CA).

R. v. *Burke*, 2015 SKPC 173.

R. v. *Caron*, 2011 BCCA 56.

R. v. *Chukwu*, 2016 SKCA 6.

R. v. *Craig*, 2016 BCCA 154.

R. v. *Cusick*, 2015 ONSC 6739.

R. v. *Duff,* 2010 ONCJ 493.

R. v. *Edwards*, [1999] O.J. No. 3819.

R. v. *Edwards*, 2015 ONCJ 347.

R. v. *Frieburg (T.L.)*, 2013 MBCA 40.

R. v. *Giles*, 2007 BCSC 1147.

R. v. *Heisler*, 1984 ABCA 30.

R. v. *H.T.*, 2010 MBPC 8.

R. v. *Jones*, 2011 ONCA 632.

R. v. *Kelsy*, 2011 ONCA 605.

R. v. *Knight*, 2008 NLCA 67.

R. v. *Kramshoj*, 2017 ONSC 2951.

R. v. *Mayo*, 2016 ONSC 125.

R. v. *Middleton*, 2000 BCCA 660.

R. v. *Nova Scotia (Ombudsman)*, 2016 NSSC 273.

R. v. *Nurse and Plummer*, 2014 ONSC 1779.

R. v. *Nurse and Plummer*, 2014 ONSC 5989.

R. v. *Pratchett*, 2016 SKPC 19.

R. v. *Rafferty*, 2012 ONSC 703.

R. v. *Sipes*, 2011 BCSC 1763.

R. v. *Smith*, 2017 ONSC 4683.

R. v. *Sonne*, 2012 ONSC 584.

R. v. *Sonne*, 2012 ONSC 2126.

R. v. *Stemberger*, 2012 ONCJ 31.

R. v. *Tuduce*, 2014 ONCA 547.

R. v. *Twitchell*, 2010 ABQB 693.

R. v. *Weir*, 2001 ABCA 181.

R. v. *Wilson*, 2014 BCSC 663.

R. v. *Witen*, 2010 ONSC 388.

R. v. *Young*, 2012 ONCJ 716.

Schreiber c. *Canada*, [1998] 1 R.C.S. 841.

Shooner c. *R.*, 2012 QCCQ 12674.

Société Télé-Mobile c. *Ontario*, [2008] 1 R.C.S. 305.

Thomson Newspapers Ltd. c. *Canada (Directeur des enquêtes et recherche, Commission sur les pratiques restrictives du commerce)*, [1990] 1 R.C.S. 425.

Tremblay c. *R.*, 2003 QCCA 72060.

Uber Canada inc. c. *Agence du revenu du Québec*, 2016 QCCS 2158.

Winnipeg Police Service Officer (Re), 2015 MBPC 70.

Jurisprudence américaine

Couch v. *United States*, 409 U.S. 322 (1973).

Hoffa v. *United States*, 385 U.S. 293 (1966).

In re Warrant to Search a Certain E-mail Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466 (S.D.N.Y. 2014).

In re Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corp., 829 F. 3d. 197, 200-01 (2nd Cir. 2016).

Katz v. *United States*, 1967 U.S. 347.

R. v. *Waterfield*, 1963 All. E.R. 659.

Smith v. *Maryland*, 422 U.S. 735 (1979).

United States v. *Miller*, 425 U.S. 435 (1976).

BIBLIOGRAPHIE

Monographies et recueils

BARBARA, J. J., Handbook of digital and multimedia evidence, Totowa, Humana, 2007.

BÉLIVEAU, P. et M. VAUCLAIR, Traité général de preuve et de procédure pénales, 20e éd., Cowansville, Éditions Yvon Blais, 2013.

BLANCHETTE, F., L'expectative raisonnable de vie privée et les principaux contextes de communications dans Internet, Mémoire de maîtrise, Université de Montréal, 2001.

COUGHLAN, S. G., Criminal procedure, Third edition, coll. Essentials of Canadian law, Toronto, Ontario, Canada, Irwin Law, 2016.

FONTANA, J. A., The Law of Search Warrants in Canada, Toronto, Butterworths, 1974.

FONTANA, J. A. et D. KEESHAN, The law of search and seizure in Canada, 9e éd., Toronto, LexisNexis, 2015.

LILLARD, T. (dir.), Digital forensics for network, Internet, and cloud computing: a forensic evidence guide for moving targets and data, Burlington, MA, Syngress, 2010.

STUART, D. et T. QUIGLEY, Learning Canadian criminal procedure, 2016.

ZEIGLER, A. D. et E. F. ROJAS, Preserving electronic evidence for trial: a team approach to the litigation hold, data collection, and evidence preservation, Boston, Elsevier, 2016.

Articles de revue et études d'ouvrages collectifs

ATRENS, J., « A Comparison of Canadian and American Constitutional Law Relating to Search and Seizure », (1994) 1 *Southwest. J. Law Trade Am.* 29.

AUSTIN, L. M., « Information Sharing and the "Reasonable" Ambiguities of Section 8 of the Charter », (2007) 57 *U Tor. LJ* 499.

« Is Consent the Fondation of Fair Information Practices? Canada's Experience under PIPEDA », 56 *Univ Tor. LJ* 181.

BARNHILL, D. S., « Cloud Computing and Stored Communications: Another look at Quon v. Arch Wireless », (2010) 25 *Berkeley Technol. Law J.* 621.

BERK, L. A., « After Jones, the Deluge: The Fourth Amendment Treatment of Information, Big Data and the Cloud », (2014) 14 *J. High Technol. Law* 1.

BRACKEN, W. J. G., « Federal Law Relating to Search and Seizure », (1974) 23 *Univ. N. B. Law J.* 53.

BRENNER, S. W., « Encryption, Smart Phones, and the Fifth Amendment », (2012) 33 *Whittier Law Rev.* 525.

BUCHAN SERAFINO, L., « "I Know My Rights, So You Go'n Need A Warrant for That": The Fourth Amendment, Riley's Impact, And Warrantless Searches of Third-Party Clouds », (2014) 19 *Berkeley J. Crim. Law* 154.

CHAN, G., « Life after Vu: Manner of Computer Searches and Search Protocols », (2014) 67 *S.C.L.R.* 433.

DALLA GUARDA, N., « Digital Encryption and the Freedom from Self-incrimination: Implications for the Future of Canadian Criminal Investigations and Prosecutions », (2014) 61 *Crim. Law Q.* 119.

DÉZIEL, P.-L. et A. STYLIOS, « La problématique des messages textes historiques : attente raisonnable de vie privée et interception de communications privées », dans Réformer le droit criminel au Canada: défis et possibilités - Criminal law reform in Canada : challenges and possibilities, Montréal, Éditions Yvon Blais, 2017, p. 536.

DYKSTRA, J. et D. RIEHL, « Forensic Collection of Electronic Evidence from Infrastructure-as-a-Service Cloud Computing », (2012) XIX *Richmond J. Law Technol.* 1.

ELLYSON, L. et EMOND, A., « Cybercriminalité : développements jurisprudentiels et perquisitions informatiques », dans *Repères*, septembre 2014, EYB2014REP1575.

FOLKINSHTEYN, B., « A Witness against Himself: A Case for Stronger Legal Protection of Encryption », (2013) 30 *St. Clara High Technol. Law J.* 414.

FRIC, A., « Reasonableness as Proportinality: Towards a Better Constructive Interpretation of the Law on Searching Computers in Canada », (2016) 21 *Appeal Rev. Curr. Law Law Reform CA* 59-82.

GOLD, A. J., « Obscured by Clouds: The Fourth Amendment and Searching Cloud Storage Accounts Through Locally Installed Software », (2015) 56 *William Mary Law Rev.* 2321.

GOLD, A. D., « Applying Section 8 in the Digital World: Seizures and Searches », (2007) ADGN/RP-211 *Alan Gold Collect. Crim. Law Artic.*

GRAY, A., « Cloud Atlas - A Map to Amending Metadata Privacy Law in the Modern Era », (2016) 52 *Gonzaga Law Rev.* 147.

HALLADAY, C. W. et J. CHAD, « A Database Too Far? Interpreting the Competition Bureau's Computer Search Powers », (2014) 27 *Can. Compet. Law Rev.* 453.

HASAN, N. R., « A Step Forward of Just a Sidestep? Year Five of the Supreme Court of Canada in the Digital Age », (2015) 71 *Supreme Court Law Rev.* 439.

HOCHHALTER, Q., « The Sky's the Limit: Twenty-First Century Searches of Hard-Drives, Smartphone Applications, & the Cloud », (2014) 90 *N. D. Law Rev.* 171.

KOHLS, S. J., « Searching the Clouds - Why Law Enforcement Officials Need to Get Their Heads Out of the Cloud and Obtain a Warrant Before Accessing a Cloud Network Account », (2012) 4 *Case West. Reserve J. Law Technol. Internet* 169.

JOHNSON, M., « Privacy in the Balance - Novel Search Technologies, Reasonable Expectations, and Recalibrating Section 8 », (2012) 58 *Crim. Law Q.* 442.

JONES, B., « Reconciling Reasonable Expectations of Privacy and Modern Technologies: U.S. v. Canadian Approaches », (2011) 83 *Crim. Rep.* 28.

JORGENSEN, L., « In Plain View: R v Jones and the Challenge of Protecting Privacy Rights in an Era of Computer Search », (2013) 46 *UBC Rev* 791.

KATTAN, I. R., « Cloudy Privacy Protections: Why the Stored Communications Act Fails to Protect the Privacy of Communications Stored in the Cloud », (2011) 13 *Vanderbilt J. Entertain. Technol. Law* 617.

KERR, O. S., « Applying the Fourth Amendment to the Internet: A General Approach », (2009) 62 *Stanford Law Rev.* 1005.

« The Case for the Third-Party Doctrine », (2009) 107 *Mich. Law Rev.* 561.

« Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data », (2015) 48 *Texas Tech Law Rev.* 1.

« Searches and seizures in a digital world », 119 *Harv. Law Rev.* 531.

KESAN, J. P., C. M. HAYES et M. N. BASHIR, « Information Privacy and Data Control in Cloud Computing: Consumers, Privacy Preferences, and Market Efficiency », (2013) 70 *Wash. Lee Law Rev.* 341.

LEIBROCK, L. R., « Duties, Support Functions, and Competencies: Digital Forensics Investigators », dans Handbook of Digital and Multimedia Forensic Evidence, Totowa, Humana Press, 2008, p. 139.

LIN, W. C., « Where Are Your Papers: The Fourth Amendment, the Stored Communications Act, the Third-Party Doctrine, the Cloud and Encryption », (2016) 65 *DePaul Law Rev.* 1093.

LOTRIONTE, N., « The Sky's the Limit - The Border Search Doctrine and Cloud Computing », (2013) 78 *Brooklyn Law Rev.* 663.

MAGOTIAUX, S., « Out of Sync: Section 8 and Technologial Advancement in Supreme Court Jurisprudence », (2015) 71 *Supreme Court Law Rev.* 501.

MARTIN, T. D., « Hey! You! Get Off of My Cloud: Defining and Protecting the Metes and Bounds of Privacy, Security and Property in Cloud Computing », (2010) 92 *J. Pat. Trademark Off. Soc.* 283.

MCCORRY, D. G., « With Cloud Technology, Who Owns Your Data? », (2014) 8 *Fed. Courts Law Rev.* 125.

MIZRAHI, S. K., « The Dangers of Sharing Cloud Storage: The Privacy Violations Suffered by Innocent Cloud Users during the Course of Criminal Investigations in Canada and the United States », (2017) 25 *Tulane J. Int. Comp. Law* 303.

MOSHIRNIA, A. V., « Separating Hard Fact from Hard Drive: A Solution for Plain View Doctrine in the Digital Domain », (2010) 23 *Harv. J. Law Technol.* 609.

NIED, M., « Cloud Computing, the Internet, and the Charter Right to Privacy: the Effect of Terms of Service Agreements on Reasonable Expectations of Privacy », (2011) 69 *Advocate Vanc. Bar Assoc.* 701.

PECORARO, A. J., « Drawing Lines in the Cloud: Implications of Extraterritorial Limits to the Stored Communications Act », (2017) 51 *Creighton Law Rev.* 75.

PELLETIER, B., « La protection de la vie privée au Canada », (2001) 35 *R.J.T.* 485-522.

PENNEY, S., « Reasonable Expectations of Privacy and Novel Search Technologies: An Economic Approach », (2007) 97 *J. Crim. Law Criminol.* 477.

« The Digitization of Section 8 of the Charter: Reform or Revolution? », (2014) 67 *S.C.L.R.* 505.

PRICE, M. W., « Rethinking Privacy: Fourth Amendment "Papers" and the Third-Party Doctrine », (2016) 8 *J. Natl. Secur. Law Policy* 247.

RASHBAUM, K. N., B. BORDEN et T. H. BEAUMONT, « Outrun the Lions: A Practical Framework for Analysis of Legal Issues in the Evolution of Cloud Computing », (2014) 12 *Ave Maria Law Rev.* 71.

RICHARDS, N., « The Third-Party Doctrine and the Future of the Cloud », (2017) 94 *Wash. Univ. Law Rev.* 1441.

ROBISON, W. J., « Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act », (2009) 98 *Georgetown Law J.* 1195.

ROTHMAN, J., « Sneak and Peek Warrants », (2001) *Alan Gold Collect. Crim. Law Artic*. 356.

SCANLAN, D. M., « Issues in digital evidence and privacy: Enhanced expectations of privacy and appellate lag times », (2012) 16 *Can. Crim. Law Rev.* 301.

SMALL, J. M., « Storing Documents in the Cloud: Toward an Evidentiary Privilege Protecting Papers and Effects Stored on the Internet », (2013) 23 *George Mason Univ. Civ. Rights Law J.* 255.

SOGHOIAN, C., « Caught in the Cloud: Privacy, Encryptions, and Government Back Doors in the Web 2.0 Era », (2010) 8 *J. Telecommun. High Technol. Law* 359.

STRIBOPOULOS, J., « A Failed Experiment? Investigative Detention: Ten Years Later » (2003), 41 *Alta. L. Rev.* 335.

STRINGHAM, J. A. Q., « Reasonable Expectations Reconsidered: A Return to the Search for a Normative Core for Section 8? », (2005) 23 *Crim. Rep.* 245.

TAYLOR, S. B., « Can You Keep a Secret: Some Wish to Ban Encryption Technology for Fears of Data Going Dark », (2016) 19 *SMU Sci. Technol. Law Rev.* 215.

TERZIAN, D., « The Fifth Amendment, Encryption, and the Forgotten State Interest », (2013) 61 *UCLA Law Rev. Discourse* 298.

« The Micro-Hornbook on the Fifth Amendment and Encryption », 104 *Georgetown Law J.* 168.

VAN HOBOKEN, J. V. J., « Privacy and Security in the Cloud: Some Realism about Technical Solutions to Transnational Surveillance in the Post-Snowden Era », (2014) 66 *Maine Law Rev.* 487.

W. BRENNER, S., « Law, Dissonance, and Remote Computer Searches », (2012) 24 *N. C. Journal Law Technol*. 43.

WILSON, S., « Compelling Passwords from Third Parties: Why the Fourth and Fifth Amendments Do Not Adequately Protect Individuals When Third Parties Are Forced to Hand over Passwords », (2015) 30 *Berkeley Technol. Law J.* 1.

WISEMAN, T. A., « Encryption, Forced Decryption, and the Constitution », (2015) 11 *J. Law Policy Inf. Soc.* 525.

YOUNG, A., « All Along the Watchtower: Arbitrary Detention and the Police Function » (1991), 29 *Osgoode Hall L.J.* 329.

Pages Internet

AMAZON, « AWS Customer Agreement », Amazon Web Services, Inc., en ligne : <https://aws.amazon.com/agreement/> (consulté le 15 mai 2018).

« What is AWS? - Amazon Web Services », Amazon Web Services, Inc., en ligne : <https://aws.amazon.com/what-is-aws/> (consulté le 30 avril 2018).

APPLE, « iCloud Terms and Conditions », Apple Legal, en ligne : <https://www.apple.com/legal/internet-services/icloud/en/terms.html> (consulté le 15 mai 2018).

APPRENDA, « IaaS, PaaS, SaaS (Explained and Compared) », Apprenda, en ligne : <https://apprenda.com/library/paas/iaas-paas-saas-explained-compared/> (consulté le 30 avril 2018).

B., G., « Choosing the Right Cloud Service: IaaS, PaaS, or SaaS », Ruby Garage, en ligne : <https://rubygarage.org/blog/iaas-vs-paas-vs-saas> (consulté le 30 avril 2018).

BACKUPIFY, « Bits & Bytes: A History of Data Storage », en ligne : <https://www.backupify.com/history-of-data-storage/> (consulté le 30 avril 2018).

CANADIAN INTERNET REGISTRATION AUTHORITY, « Internet use in Canada », Canadian Internet Registration Authority (CIRA) (2 décembre 2016), en ligne : <https://cira.ca/factbook/domain-industry-data-and-canadian-Internet-trends/internet-use-canada> (consulté le 20 octobre 2017).

CCM, « Trouver son adresse MAC » (mars 2018), en ligne : <http://www.commentcamarche.com/faq/10935-trouver-son-adresse-mac> (consulté le 31 mars 2018).

COLUMBUS, L., « Roundup Of Cloud Computing Forecasts, 2017 », en ligne : <https://www.forbes.com/sites/louiscolumbus/2017/04/29/roundup-of-cloud-computing-forecasts-2017/#5d7958b731e8> (consulté le 20 octobre 2017).

COMMISSAIRE À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, « Des données au bout des doigts : La biométrie et les défis qu'elle pose à la protection de la vie privée » (1 novembre 2011), en ligne : <https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/renseignements-sur-la-sante-renseignements-genetiques-et-autres-renseignements-sur-le-corps/gd_bio_201102/> (consulté le 14 avril 2018).

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, « Projet de loi C-13, Loi sur la protection des Canadiens contre la cybercriminalité - Mémoire présenté au Comité sénatorial permanent des affaires juridiques et constitutionnelles » (19 novembre 2014), en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/conseils-au-parlement/2014/parl_sub_141119/> (consulté le 17 novembre 2016).

DANIEL, L. E., « Plain View Doctrine in Digital Evidence Cases—A Common Sense Approach », Forensic Magazine (23 octobre 2009), en ligne : <https://www.forensicmag.com/article/2009/10/plain-view-doctrine-digital-evidence-cases%E2%80%94-common-sense-approach> (consulté le 13 avril 2018).

DROPBOX, « Terms », Dropbox, en ligne : <https://www.dropbox.com/privacy> (consulté le 15 mai 2018).

FOLEY, M. J., « Microsoft bullish on Congress' inclusion of CLOUD Act in funding bill », ZDNet, en ligne : <https://www.zdnet.com/article/microsoft-bullish-on-congress-inclusion-of-cloud-act-in-funding-bill/> (consulté le 20 mai 2018).

GOOGLE, « Terms of Service – Privacy & Terms », en ligne : <https://policies.google.com/terms> (consulté le 15 mai 2018).

GREENBERG, A., « Who Reads The Fine Print Online? Less Than One Person In 1000 », Forbes, en ligne : <https://www.forbes.com/sites/firewall/2010/04/08/who-reads-the-fine-print-online-less-than-one-person-in-1000/> (consulté le 15 mai 2018).

HOSENBALL, M., « FBI paid under $1 million to unlock San Bernardino iPhone: sources », Reuters (4 mai 2016), en ligne : <https://www.reuters.com/article/us-apple-encryption/fbi-paid-under-1-million-to-unlock-san-bernardino-iphone-sources-idUSKCN0XQ032> (consulté le 14 avril 2018).

IBM, « IaaS PaaS SaaS Cloud Service Models », IBM, en ligne : <https://www.ibm.com/cloud/learn/iaas-paas-saas> (consulté le 30 avril 2018).

INSTITUT DE LA STATISTIQUE DU QUÉBEC, « Part des entreprises branchées qui utilisent l'infonuagique, Québec, 2012 et 2016 », en ligne : <http://www.stat.gouv.qc.ca/statistiques/science-technologie-innovation/utilisation-internet/entreprises/utilisation-infonuagique.html> (consulté le 9 mai 2018).

IP LOCATION, « What is my IP address? », en ligne : <https://www.iplocation.net/find-ip-address> (consulté le 31 mars 2018).

KHARPAL, A., « Apple vs FBI: All you need to know » (29 mars 2016), en ligne : <https://www.cnbc.com/2016/03/29/apple-vs-fbi-all-you-need-to-know.html> (consulté le 14 avril 2018).

KUMAR, M., « FBI Director — You Should Cover Your Webcam With Tape », The Hacker News, en ligne : <https://thehackernews.com/2016/09/hacking-webcam-cover.html> (consulté le 9 avril 2018).

MAK, A., « Congress Put the Controversial CLOUD Act in Its Spending Bill. What Does That Mean For Data Privacy? », Slate Magazine (22 mars 2018), en ligne : <https://slate.com/technology/2018/03/cloud-act-microsoft-justice-department-omnibus-spending-bill.html> (consulté le 20 mai 2018).

MELL, P. et T. GRANCE, « The NIST Definition of Cloud Computing », Computer security resource center, en ligne : <https://csrc.nist.gov/publications/detail/sp/800-145/final> (consulté le 30 avril 2018).

MICROSOFT, « Ensuring Data Integrity with Hash Codes », en ligne : <https://docs.microsoft.com/en-us/dotnet/standard/security/ensuring-data-integrity-with-hash-codes> (consulté le 31 mars 2018).

« Public Cloud vs Private Cloud vs Hybrid Cloud », Microsoft Azure, en ligne : <https://azure.microsoft.com/en-gb/overview/what-are-private-public-hybrid-clouds/> (consulté le 30 avril 2018).

« Services Agreement », en ligne : <https://www.microsoft.com/en-ca/servicesagreement/> (consulté le 15 mai 2018).

MOZY, « Online Backup Storage and Software for photos, music, and docs », en ligne : <https://mozy.com/product/mozy/personal> (consulté le 15 mai 2018).

« Privacy Statement », en ligne : <https://mozy.com/about/legal/privacy> (consulté le 15 mai 2018).

NELSON, T., « Setup and Price Guide to Google Drive for the Mac », Lifewire, en ligne : <https://www.lifewire.com/how-to-set-up-and-use-google-drive-on-mac-2260845> (consulté le 17 mai 2018).

NICOL, J. et D. VALIQUET, « Résumé législatif du projet de loi C-13 : Loi modifiant le Code criminel, la Loi sur la preuve au Canada, la Loi sur la concurrence et la Loi sur l'entraide juridique en matière criminelle », en ligne : <http://www.bdp.parl.gc.ca/content/lop/LegislativeSummaries/41/2/c13-f.pdf> (consulté le 8 novembre 2016).

OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE « Chiffrement » (2013), en ligne : <https://www.oqlf.gouv.qc.ca/ressources/bibliotheque/dictionnaires/terminologie_sec_informatique/chiffrement.html> (consulté le 25 septembre 2018).

« infonuagique » (2017), en ligne : <http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=26501384> (consulté le 20 octobre 2017).

PEARSON, J., et J. LING, « Exclusive: How Canadian Police Intercept and Read Encrypted BlackBerry Messages », *Motherboard* (14 avril 2016), en ligne: <https://motherboard.vice.com/en_us/article/mg77vv/rcmp-blackberry-project-clemenza-global-encryption-key-canada> (consulté le 25 septembre 2018);

RATHNAM, L., « PRISM, Snowden and Government Surveillance: 6 Things You Need to Know », *Cloudwards* (29 mars 2017), en ligne : <https://www.cloudwards.net/prism-snowden-and-government-surveillance/> (consulté le 25 septembre 2018).

VERMEYS, N., J. M. GAUTHIER et S. K. MIZRAHI, « Étude sur les incidences juridiques de l'utilisation de l'infonuagique par le gouvernement du Québec », en ligne : <https://www.vermeys.com/publications/etude-sur-les-incidences-juridiques-de-lutilisation-de-linfonuagique-par-le-gouvernement-du-quebec/> (consulté le 25 septembre 2018).

SEABY, K. et R. MANGAT, « Making Privacy Meaningful in a Digital Age », British Columbia Civil Liberties Association (15 décembre 2014), en ligne : <https://bccla.org/2014/12/making-privacy-meaningful-in-a-digital-age/> (consulté le 9 avril 2018).

SPIDEROAK, « No Knowledge, Secure-by-Default Products », en ligne : <https://spideroak.com/no-knowledge/> (consulté le 15 mai 2018).

« Privacy Policy », SpiderOak, en ligne : <https://spideroak.com/privacy-policy/> (consulté le 15 mai 2018).

STATISTA, « Consumer cloud computing user worldwide 2018 », Statista, en ligne : <https://www.statista.com/statistics/321215/global-consumer-cloud-computing-users/> (consulté le 9 mai 2018).

U.S. DEPARTMENT OF THE INTERIOR, « The Cloud First Strategy » (23 août 2017), en ligne : <https://www.doi.gov/cloud/strategy> (consulté le 10 mai 2018).

WHITE, J., « Private vs. Public Cloud: What's the Difference? », Expedient (5 juin 2014), en ligne : <https://www.expedient.com/blog/private-vs-public-cloud-whats-difference/> (consulté le 30 avril 2018).

WIKIPEDIA, « Infrastructure as a service », dans Wikipédia, en ligne : <https://fr.wikipedia.org/w/index.php?title=Infrastructure_as_a_service&oldid=143431424> (consulté le 30 avril 2018).

« BlackBerry Messenger », dans Wikipedia, en ligne : <https://en.wikipedia.org/w/index.php?title=BlackBerry_Messenger&oldid=829127329> (consulté le 12 avril 2018).

« Keystroke logging », dans Wikipedia, en ligne : <https://en.wikipedia.org/w/index.php?title=Keystroke_logging&oldid=831183322> (consulté le 14 avril 2018).

« Cloud computing », dans Wikipédia, en ligne : <https://fr.wikipedia.org/w/index.php?title=Cloud_computing&oldid=147706181> (consulté le 30 avril 2018).

« Internet des objets », dans Wikipédia, en ligne : <https://fr.wikipedia.org/w/index.php?title=Internet_des_objets&oldid=147938653> (consulté le 22 mai 2018).

ZORABEDIAN, J., « Police say they can read Blackberry PGP encrypted email », *Naked Security* (13 janvier 2016), en ligne : <https://nakedsecurity.sophos.com/2016/01/13/police-say-they-can-crack-blackberry-pgp-encrypted-email/> (consulté le 25 septembre 2018).

« GPS: The Global Positioning System », en ligne : <https://www.gps.gov/> (consulté le 31 mars 2018).

« Mémoire : Projet de loi C 13, Loi sur la protection des Canadiens contre la cybercriminalité - Le 19 novembre 2014 - Commissariat à la protection de la vie privée du Canada », en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/conseils-au-parlement/2014/parl_sub_141119/> (consulté le 13 juin 2017).

« What is metadata? - Definition from WhatIs.com », WhatIs.com, en ligne : <http://whatis.techtarget.com/definition/metadata> (consulté le 31 mars 2018).

Annexe I

Résumé des différentes ordonnances de communication prévues au Code criminel[606]

Pouvoir d'enquête	**Exemple de données *obtenues***	**Seuil**
Ordre de préservation – 21 jours (art. 487.012)	Aucune donnée	Soupçon
Ordonnance de préservation – trois mois (art. 487.013)	Aucune donnée	Soupçon
Ordonnance générale de communication (art. 487.014)	Toute donnée stockée	Croyance
Ordonnance de communication en vue de retracer une communication donnée (art. 487.015)	Adresse de courriel, de protocole Internet (IP) ou MAC	Soupçon
Ordonnance de communication : données de transmission (art. 487.016)	Adresse d'IP, domaines et pages de sites Web visités, protocoles de partage de fichiers et autres, numéros de paquets, termes de recherche dans les moteurs de recherche et adresse de courriel	Soupçon
Ordonnance de communication : données de localisation (art. 487.017)	Données de localisation et coordonnées GPS	Soupçon
Ordonnance de communication : données financières (art. 487.018)	Renseignements sur le titulaire du compte, types de compte, date de création du compte et adresse courante	Soupçon
Mandat pour un dispositif de localisation : opération ou chose (par. 492.1[1])	Lieux d'utilisation de la carte de crédit ou bancaire et mouvements de véhicules	Soupçon
Mandat pour un dispositif de localisation : personne physique (par. 492.1[2])	Lieu de la personne physique localisée (grâce à un appareil mobile personnel)	Croyance
Mandat pour un enregistreur de données de transmission (art. 492.2)	Voir ci-dessus	Soupçon

[606] « Mémoire : Projet de loi C 13, Loi sur la protection des Canadiens contre la cybercriminalité - Le 19 novembre 2014 - Commissariat à la protection de la vie privée du Canada », en ligne : <https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/conseils-au-parlement/2014/parl_sub_141119/> (consulté le 13 juin 2017).